UNIVERSIDAD NACIONAL DE PIURA

FACULTAD DE INGENIERIA INDUSTRIAL

ESCUELA PROFESIONAL DE INGENIERÍA INFORMÁTICA

"PROPUESTA DE UN MODELO DE AUDITORÍA DE SISTEMAS DE INFORMACIÓN PARA ENTIDADES PÚBLICAS"

PRESENTADO POR: BR. LUIS ERICK POMA JULCA

ASESOR: MBA. PERSI WILLIANSH CABRERA ANTÓN

LÍNEA DE INVESTIGACIÓN: INFORMÁTICA, ELECTRÓNICA Y TELECOMUNICACIONES

SUB LÍNEA DE INVESTIGACIÓN: COMPUTACIÓN

PIURA-PERÚ

2019

UNIVERSIDAD NACIONAL DE PIURA

FACULTAD DE INGENIERIA INDUSTRIAL

ESCUELA PROFESIONAL DE INGENIERÍA INFORMÁTICA

INFORME FINAL DE TESIS

"PROPUESTA DE UN MODELO DE AUDITORÍA DE SISTEMAS DE INFORMACIÓN PARA ENTIDADES PÚBLICAS"

LUIS ERICK POMA JULCA

AUTOR

MBA. CABRERA ANTON PERSI WILLIANSH

ASESOR

DECLARACIÓN JURADA DE ORIGINALIDAD DE LA TESIS

Yo, **LUIS ERICK POMA JULCA**, identificado con **DNI Nº 41879740**., Bachiller de la ESCUELA PROFESIONAL DE INGENIERÍA INFORMÁTICA de la Facultad de INGENIERÍA INDUSTRIAL, y domiciliado en Urb. San Ramón Mza. C2 lote 18, del Distrito de Piura, Provincia de Piura, Departamento de Piura.

Celular:960308964

Email: luchitopj051@hotmail.com

"PROPUESTA DE UN MODELO DE AUDITORIA DE SISTEMAS DE INFORMACION PARA ENTIDADES PUBLICAS"

DECLARO BAJO JURAMENTO: que el informe de investigación que presento es original e inédita, no siendo copia parcial ni total de una tesis desarrollada, y/o realizada en el Perú o en el Extranjero, en caso contrario de resultar falsa la información que proporciono, me sujeto a los alcances de lo establecido en el Art. Nº 411, del código Penal concordante con el Art. 32º de la Ley Nº 27444, y Ley del Procedimiento Administrativo General y las Normas Legales de Protección a los Derechos de Autor. En fe de lo cual firmo la presente.

Piura, 05 de febrero del 2019

Br. Luis Erick Poma Julca
DNI Nº 41879740

Artículo 411.- El que, en un procedimiento administrativo, hace una falsa declaración en relación con hechos o circunstancias que le corresponde probar, violando la presunción de veracidad establecida por ley, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años.

Art. 4. Inciso 4.12 del Reglamento del Registro Nacional de Trabajos de Investigación para optar grados académicos y títulos profesionales –RENATI Resolución de Consejo Directivo Nº 033-2016-SUNEDU/CD.

UNIVERSIDAD NACIONAL DE PIURA

FACULTAD DE INGENIERIA INDUSTRIAL

ESCUELA PROFESIONAL DE INGENIERÍA INFORMÁTICA

INFORME FINAL DE TESIS

"PROPUESTA DE UN MODELO DE AUDITORÍA DE SISTEMAS DE INFORMACIÓN PARA ENTIDADES PÚBLICAS"

JURADO AD HOC

DR. HUGO VICTOR ROSALES GARCÍA

PRESIDENTE

MG. YOLANDA ESTHER LIZANA PUELLES

SECRETARIA

ING. ARTURO SANDOVAL RIVERA

VOCAL

4

UNIVERSIDAD NACIONAL DE PIURA
FACULTAD DE INGENIERÍA INDUSTRIAL
DECANATO

ACTA DE EVALUACIÓN Y SUSTENTACIÓN DE TESIS

Expediente N° 1554 / 2017

Los miembros del Jurado Calificador Ad-Hoc de la Sustentación de Tesis nombrado con Resolución N° **035-CF-FII-UNP-18** de fecha 12/01/2018 que suscriben, se reunieron en acto público en la sala de exposiciones de la Facultad de Ingeniería Industrial de la Universidad Nacional de Piura, el día **08 de Julio del 2019** a las **12:00 pm**, para evaluar la defensa de la Tesis titulada **"PROPUESTA DE UN MODELO DE AUDITORÍA DE SISTEMAS DE INFORMACIÓN PARA ENTIDADES PÚBLICAS"**, presentada por el Bachiller **LUIS ERICK POMA JULCA** y asesorado por el **MBA. PERSI WILLIANSH CABRERA ANTÓN** .

Después de haber calificado el Informe Final de la Tesis, escuchada la sustentación y las respuestas a las preguntas formuladas por el Jurado, se le declara .....APROBADO..... para optar el Título de **INGENIERO INFORMÁTICO** con el puntaje de ..64... que corresponde al calificativo de .....BUENO.....

Jurado / Calificación	Presidente	Secretario	Vocal	Puntaje Promedio
Documento (Max 60 puntos)	34	34	34	34
Sustentación (Max 40 puntos)	30	30	30	30
PUNTAJE TOTAL				64

En consecuencia, el sustentante queda en condición de recibir el Título Profesional que se indica, conferido por el Consejo Universitario de la Universidad Nacional de Piura de conformidad con las Normas Estatutarias y la Ley Universitaria en vigencia.

Ciudad Universitaria, 08 de Julio del 2019

Dr. HUGO VICTOR ROSALES GARCÍA	MSc. ESTHER YOLANDA LIZANA PUELLES	Ing. ARTURO SANDOVAL RIVERA
PRESIDENTE	**SECRETARIO**	**VOCAL**

DEDICATORIA

Esta tesis se la dedico a mi Padre Dios quien supo guiarme por buen camino, darme fuerzas para seguir adelante y no desmayar en los problemas que se me presentaban, enseñándome a encarar las adversidades sin perder nunca la dignidad ni desfallecer en el intento.

A mis padres quienes por ellos soy lo que soy, a mi mamita Anita Marlene Julca Vicente y a mi papá Irenio A. Poma Morocho, por su apoyo, consejos, comprensión, amor, ayuda en los momentos difíciles y por ayudarme con los recursos necesarios para poder estudiar. Me han dado todo lo que soy como persona, mis valores, mis principios, mi carácter, mi empeño y mi perseverancia para conseguir mis objetivos.

Atte. Luis Erick Poma Julca.

AGRADECIMIENTO

En primer lugar agradezco a mi Padre Dios por permitirme llegar a este punto de mi vida profesional.

Agradecer también a mis padres por su infinito e incondicional apoyo para culminar cada etapa de mi vida, por haberme proporcionado la mejor educación y lecciones de vida. En especial a mi mamita Anita por haberme enseñado que con esfuerzo, trabajo y constancia todo se consigue y que en esta vida nadie te regala nada.

A mis amigos y compañeros de clase por siempre estar a mi lado.

Agradezco también a mis formadores, personas integras de gran sabiduría quienes se han esforzado por llegar al punto en el que me encuentro.

Y de manera especial agradezco a mi asesor el ingeniero Persi Cabrera por su tiempo y dedicación y valga la redundancia para asesorarme de la mejor y correcta manera posible para poder terminar con éxito mi tesis.

ÍNDICE GENERAL

RESUMEN

Con el presente trabajo de investigación se ha desarrollado un modelo para poder realizar auditorías de sistemas de información en las entidades públicas, este modelo propuesto puede ser utilizado por los ingenieros informáticos y/o de sistemas que se dedican al desarrollo de auditorías de este tipo. Para el estudio se utilizó una metodología con enfoque cuantitativo, porque la auditoria se desarrolla sobre hechos objetivos cuantificables, el nivel del trabajo realizado es descriptivo, porque lo que se busca es apoyar con una herramienta efectiva al auditor en el proceso de auditoría de sistemas, de esta forma evalúa los controles de los sistemas de información y las tecnologías relacionadas de una manera eficaz, de tal modo que las evidencias encontradas, sustenten los hallazgos y deficiencias de los asuntos auditados, razón por la cual se ha descrito de forma detallada todos los procedimientos, técnicas y pruebas de auditoría que se pueden utilizar con la aplicación del modelo propuesto. La auditoría por su naturaleza se aplica sobre asuntos determinados de forma objetiva, y las evidencias se recogen tal como se encuentran, de acuerdo a lo anterior, se infiere que, al no existir una manipulación del asunto auditado, lo idóneo ha sido plantear el presente trabajo como un diseño no experimental. Finalmente, podemos asegurar que se ha hecho un nuevo aporte al conocimiento con el desarrollo del modelo propuesto.

Palabras claves: modelo de auditoría de sistemas, procedimientos, técnicas, evidencias, deficiencias, hallazgos.

ABSTRACT

With the present research work, a model has been developed to perform audits of information systems in public entities, this proposed model can be used by computer engineers and / or systems that are dedicated to the development of audits of this type. For the study, a methodology with a quantitative approach was used, because the audit is carried out on quantifiable objective facts, the level of the work done is descriptive, because what is sought is to support the auditor in the systems audit process with an effective tool, In this way, it evaluates the controls of the information systems and the related technologies in an effective way, in such a way that the evidences found support the findings and deficiencies of the audited matters, which is why all the information has been described in detail. procedures, techniques and audit tests that can be used with the application of the proposed model. The audit by its nature is applied on certain matters objectively, and the evidence is collected as they are, according to the above, it is inferred that there is no manipulation of the matter audited, it has been appropriate to raise the present work as a non-experimental design. Finally, we can assure that a new contribution to knowledge has been made with the development of the proposed model.

Keywords: audit model of systems, procedures, techniques, evidences, deficiencies, findings.

INTRODUCCIÓN

La información en la empresa pública o privada es uno de los activos más importantes y de mayor valor que posee, y, por ende, se deberían desarrollar mecanismos de control y auditoría que le permita a la organización asegurar la integridad, efectividad, eficiencia, confidencialidad, disponibilidad, confiabilidad y cumplimiento de la información.

Las instituciones públicas del país en su mayoría cuentan con sistemas de información, sin embargo, el órgano de control institucional en la mayoría de ellas, no incluye en sus planes de trabajo o no dan la importancia debida a realizar acciones de control o de auditoría sobre los sistemas de información, los factores son varios y se mencionan en la problemática. Esta falta de control y auditoría ocasiona perjuicio a la institución específicamente en el activo de la información afectando sus características de calidad señaladas en el párrafo anterior.

Es por eso que la propuesta de desarrollar un modelo de auditoría de sistemas de información basado en la normatividad vigente dictada por la Contraloría General de la República (ente rector del sistema) y relacionadas como la Norma Técnica Peruana 17799, el modelo recoge aspectos importantes y relevantes de marcos de referencia de auditoría, como COBIT 4.1 y la ISO 27001, dicho modelo será de valiosa ayuda para el órgano de control interno de las instituciones públicas, y, los auditores independientes, quienes contarán con instrumentos y herramientas que podrán utilizar para llevar a cabo acciones de control y auditoría frente a alguna situación presentada que puede poner en riesgo la calidad de la información.

CAPÍTULO I
ASPECTOS DE LA PROBLEMÁTICA

1.1. DESCRIPCIÓN DE LA REALIDAD PROBLEMÁTICA

El avance tecnológico de las Tecnologías de Información y Comunicación (TIC) ha escalado varios niveles en el mundo y en el país, según el Informe global de Tecnología de la Información 2016 (World Economic Forum 2016) manifiesta: que *"La edición 2016 bajo el lema: "Innovar en la economía digital", mide a 139 economías, Perú se encuentra significativamente rezagado en términos de aprovechamiento de las TIC para modernizar su economía nacional. Los insuficientes avances en el desarrollo de la infraestructura nacional de TIC (puesto 86) se han traducido en un estancamiento relativo de las TIC. La mala calidad de su sistema educativo (puesto 129), la baja calidad de la educación en matemáticas y ciencias (136), falta de eficacia de los órganos legislativos (138) y poca eficiencia del sistema legal en la solución de conflictos (129) son factores que están obstaculizando la capacidad del país para obtener mayores impactos económicos y permitir que la economía nacional se enfoque en la transición hacia actividades de mayor valor añadido".*

Con los datos descritos en el párrafo anterior podemos apreciar la magnitud del problema de las TIC que se presentan en las empresas e instituciones públicas del Perú, por eso es importante hacer una propuesta de un modelo de auditoría de sistemas para contribuir con los órganos de control interno y los especialistas de auditoría de sistemas, para realizar las acciones de control que tienen como finalidad hacer notar estas deficiencias en las instituciones con referencia al uso e implementación de las TIC.

Los entes públicos del Estado Peruano no pueden hacer control y auditoría efectiva sobre sus sistemas de información por varios factores: Como primer factor, no contar con personal idóneo que tenga los conocimientos y experiencia suficiente en el tema de las TIC, un segundo factor es, no incluir en sus planes anuales acciones de control y auditoría sobre las TIC y como tercer factor, no tener un horizonte claro sobre cómo hacer una auditoría o ejercer control a los sistemas de información que poseen, esto debido a que

el ente rector del sistema nacional de control (Contraloría General de la República) no ha desarrollado una metodología, una guía o modelo para realizar acciones control y auditoría de sistemas de información.

Ante esta situación presentada, se pretende ayudar en la solución con la elaboración de un modelo de auditoría de sistemas de información para que los profesionales del órgano de control interno, sociedades de auditoría y auditores independientes relacionados, lo tomen para que lo puedan incluir en de forma correcta en sus actividades de control y auditorías de sistemas.

1.2. FORMULACIÓN DEL PROBLEMA:

¿En qué medida la propuesta de un modelo de auditoría de sistemas ayudará a las acciones de control en una auditoría de TIC para una entidad pública?

1.3. JUSTIFICACIÓN E IMPORTANCIA DE LA INVESTIGACIÓN:

El presente trabajo de investigación se justifica porque existe un problema en las entidades públicas, que es la falta de control y auditoría en los sistemas de información que administran, existe un desinterés o desconocimiento por parte de los funcionarios sobre las tecnologías de información, afectándose directamente los atributos de la calidad de la información, la cual es producida en su mayor proporción por los sistemas de información, siendo éste un problema a nivel Nacional.

La presentación de este trabajo de investigación es importante, porque se pretende proponer un modelo de auditoría de sistemas, para ayudar a los órganos de control interno y especialistas de auditoría de sistemas, con

herramientas que permitan desarrollar de forma más adecuada las acciones de control sobre los sistemas de información de las empresas públicas. También se busca que los órganos de control interno a través de sus profesionales de informática de dichas instituciones optimicen su plan de anual de auditoría, tomando como referencia el modelo de auditoría de sistemas de información propuesto.

1.4. OBJETIVOS

1.4.1. OBJETIVO GENERAL

Proponer un modelo de auditoría de sistemas de información que ayude a las acciones de control en una auditoría de TIC para una entidad pública.

1.4.2. OBJETIVOS ESPECÍFICOS

- Conocer la organización pública de forma general, sus normas, políticas y procedimientos más importantes relacionados a los sistemas de información.
- Establecer los objetivos del modelo de auditoría propuesto.
- Establecer los objetivos de control y los procedimientos de auditoría a aplicar sobre los sistemas de información en las instituciones públicas.
- Determinar el programa de auditoría donde se especifican los procedimientos de auditoría.
- Especificar las pruebas de software en los procedimientos de auditoría que correspondan.

1.5. DELIMINTACIÓN DE LA INVESTIGACIÓN

La investigación se delimita desarrollar un modelo de auditoría de sistemas de información para aplicarlo en auditorías de sistemas sobre entidades públicas, de acuerdo a la normatividad vigente a la fecha actual, que rige al sector público. También se tiene como delimitación, el ámbito de aplicación para los cuestionarios, los cuales serán aplicados sobre las empresas públicas de Piura.

CAPÍTULO II
MARCO TEÓRICO

2.1. ANTECEDENTES DE LA INVESTIGACIÓN

- ALIAGA, L. (2013); En su tesis denominada **"Diseño de un Sistema de Gestión de Seguridad de Información para un Instituto Educativo"** tiene como objetivo diseñar un Sistema de Gestión de Seguridad de Información (SGSI) basado en las normas internacionales ISO/IEC 27001:2005 e ISO/IEC 27002:2005, adoptando como framework de negocios la actual versión de COBIT. Para el diseño de un SGSI, la norma ISO 27001 adopta el ciclo de Deming como metodología, el cual se puede aplicar a todos los procesos que abarca el SGSI. Dicha metodología es más conocida por sus siglas en inglés como PDCA: Plan-Do-Check-Act. Como resultados se tiene el modelamiento de los procesos de negocio, el Inventario de los activos de información críticos del instituto educativo relacionados a los procesos de negocios del alcance del SGSI, el Mapa de los riesgos de la seguridad de información a los que los activos críticos identificados están expuestos y la lista de controles que permitan gestionar los riesgos identificados en los activos críticos del instituto educativo.

- BARAHONA, J. (2014); La presente tesis titulada **"Auditoria de los riesgos informáticos en el Departamento de Tecnología de la empresa KUBIEC usando COBIT 4.1 y la Norma ISO/IEC 27001 como marco de referencia"** como objetivo plantea determinar los riesgos asociados a las Tecnologías de Información y Comunicación presentes el Departamento. La metodología utilizada para la caracterización de la empresa del presente proyecto se basa en las buenas prácticas de auditoría informática. Como resultado de la tesis, se formula el diseño de un plan de seguridad basado en los controles que propone la norma ISO/IEC 27001 para gestionar los riesgos detectados.

- CORAISACA, J y LLUMIQUINGA, C (2012); En la presente tesis titulada **"Aplicación de COBIT 4.1 en la Auditoria de una aplicación informática tipo web de una Institución Financiera"** tiene como

principal objetivo, presentar los resultados de la auditoría realizada a la aplicación web de una institución financiera, utilizando las directrices de auditoría de COBIT 4.1. La metodología utilizada para la auditoría fue el marco de trabajo de COBIT 4.1. El resultado del trabajo es el informe final de auditoría que reporta los hallazgos y las recomendaciones.

- MOLINA, J & OÑA, D (2013); En su tesis denominada **"Auditoria del sistema informático de la empresa "Manufacturas Americanas CIA.LTDA"** tiene como principal objetivo, presentar los resultados de la auditoría teniendo en cuenta los dominios, procesos y objetivos de control para desarrollar un modelo de madurez. La metodología utilizada para la auditoría fue el marco de trabajo de COBIT 4.1. El resultado del trabajo es la identificación de procesos críticos y el nivel de madurez de la empresa.

2.2. BASES TEÓRICAS

2.2.1. DEFINICIÓN DE AUDITORIA

Según NTP-ISO/IEC 12207, (2006), citado por Ramos, C. (2015), auditoría es un proceso para determinar el cumplimiento con los requerimientos, planes y contrato, según aplique. Se indica además que este proceso puede ser empleado sin importar por alguna de las dos partes, donde una de ellas (la auditora) audita los productos software o actividades de la otra parte (la auditada). Según ISACA (2008), la auditoría de los sistemas de información se define como cualquier auditoría que abarca la revisión y evaluación de todos los aspectos (o de cualquier porción de ellos) de los sistemas automáticos de procesamiento de la información, incluidos los procedimientos no automáticos relacionados con ellos y las interfaces correspondientes

2.2.2. AUDITORIA INFORMÁTICA

Según Muñoz, C.; (2002), citado por Ramos, C. (2015), es la revisión técnica, especializada y exhaustiva que se realiza a los sistemas computacionales, software e información utilizados en una empresa, sean individuales, compartidos y/o de redes, así como a sus instalaciones, telecomunicaciones, mobiliario, equipos periféricos y demás componentes. Dicha revisión se realiza de igual manera a la gestión informática, el aprovechamiento de sus recursos, las medidas de seguridad y los bienes de consumo necesarios para el funcionamiento del centro de cómputo. El propósito fundamental es evaluar el uso adecuado de los sistemas para el correcto ingreso de los datos, el procesamiento adecuado de la información y la emisión oportuna de sus resultados en la institución, incluyendo la evaluación en el cumplimiento de las funciones, actividades y operaciones de funcionarios, empleados y usuarios involucrados con los servicios que proporcionan los sistemas computacionales a la empresa.

2.2.3. TIPOS DE AUDITORIAS

Una de las clasificaciones que propone Muñoz, C.; (2002), citado por Ramos, C. (2015), es:

Auditorías por su lugar de aplicación

- Auditoría externa
- Auditoría interna

Auditorías por su área de aplicación

- Auditoría financiera
- Auditoría administrativa
- Auditoría operacional
- Auditoría integral

• Auditoría gubernamental
• Auditoría de sistemas

Auditorías especializadas en áreas específicas

• Auditoría al área médica (evaluación médico-sanitaria)
• Auditoría al desarrollo de obras y construcciones (evaluación de ingeniería)
• Auditoría fiscal
• Auditoría laboral
• Auditoría de proyectos de inversión
• Auditoría a la caja chica o caja mayor (arqueos)
• Auditoría al manejo de mercancías (inventarios)
• Auditoría ambiental
• Auditoría de sistemas

Auditoría de sistemas computacionales

• Auditoría informática
• Auditoría con la computadora
• Auditoría sin la computadora
• Auditoría a la gestión informática
• Auditoría al sistema de cómputo
• Auditoría alrededor de la computadora
• Auditoría de la seguridad de sistemas computacionales
• Auditoría a los sistemas de redes
• Auditoría integral a los centros de cómputo
• Auditoría ISO-9000 a los sistemas computacionales
• Auditoría outsourcing
• Auditoría ergonómica de sistemas computacionales

2.2.4. TÉCNICAS DE AUDITORÍA

Según RC 152-98-CG, las técnicas de auditoría son métodos prácticos de investigación y prueba que utiliza el auditor para obtener evidencia necesaria que fundamenta su opinión. Las

técnicas más utilizadas al realizar al realizar pruebas de transacciones y saldos son:

1. Técnicas de Verificación Ocular
2. Técnicas de Verificación Oral
3. Técnicas de Verificación Escrita
4. Técnicas de Verificación Documental
5. Técnicas de Verificación Física

1. Técnicas de Verificación Ocular

a) **Comparación. -** Es el acto de observar la similitud o diferencia existente entre dos o más elementos. Dentro de la fase de ejecución se efectúan la comparación de resultados contra criterios aceptables facilitando de esa forma la evaluación por el auditor y la elaboración de observaciones, conclusiones y recomendaciones.

b) **Observación. -** Es el examen ocular realizado para cerciorarse como se ejecutan las operaciones. Esta técnica es de utilidad en todas las fases de la auditoria por cuyo intermedio el auditor se cerciorará de ciertos hechos y circunstancias en especial las relacionadas con la forma de ejecución de las operaciones apreciando personalmente de manera abierta o directa.

2. Técnicas de Verificación Oral

a) **Indagación. -** Es el acto de obtener información verbal sobre un asunto mediante averiguaciones directas o conversaciones con los funcionarios de la entidad. Es de especial utilidad la indagación en la auditoria cuando se examinan áreas específicas no documentadas, sin embargo,

sus resultados por si solos no constituyen evidencia suficiente.

b) **Entrevista. -** Pueden ser efectuadas al personal de la entidad auditada o personas beneficiarias de los programas o proyectos. Para obtener mejores resultados debe prepararse apropiadamente, especificar quienes serán entrevistados, definir las preguntas a formular, alertar al entrevistado acerca del propósito y puntos hacer abordados.

c) **Encuesta. -** Pueden ser útiles para recopilar información de un gran universo de datos o grupos de personas. Pueden ser enviadas por correo u otro método a las personas. Su ventaja principal radica en la economía en términos de costo y tiempo sin embrago su desventaja se manifiesta en su inflexibilidad al no obtener más de lo que se pide, lo cual en ciertos casos puede ser muy costoso.

3. Técnica de Verificación Escrita

a) **Analizar. -** Consiste en la separación y evaluación critica, objetiva y minuciosa de los elementos o partes que conforman una operación, actividad, transacción o proceso con el fin de establecer su naturaleza, su relación y conformidad con los criterios normativos y técnicos existentes. Los procedimientos de análisis están referidos a la comparación de cantidades, porcentajes y otros.

b) **Confirmación. -** Permite comprobar la autenticidad de los registros y documentos analizados a través de información directa y por escrito, otorgada por funcionarios que participan o realizan las operaciones sujetas a examen por lo que están a disposición de opinar e informar en forma válida y veraz sobre ellas.

c) **Tabulación. -** Consiste en agrupar los resultados obtenidos en áreas, segmentos o elementos examinados de manera que se facilite la elaboración de conclusiones.

d) **Conciliación. -** Implica hacer que concuerden dos conjuntos de datos relacionados, separados o independientes. Esta técnica consiste en analizar la información producida por diferentes unidades operativas o entidades, respecto de una misma operación o actividad.

4. Técnicas de Verificación Documental

a) **Comprobación. -** Se aplica en el curso de un examen con el objetivo de verificar la existencia, legalidad, autenticidad y legitimidad de las operaciones efectuadas por una entidad mediante la verificación de los documentos que las justifican.

b) **Computación. -** se utiliza para verificar la exactitud y corrección aritmética de una operación o resultado. Se prueba solamente la exactitud de un cálculo, por lo tanto, se requiere de otras pruebas adicionales para establecer la validez de los datos que forman parte de una operación.

c) **Rastreo. -** Se utiliza para dar seguimiento y controlar una operación de manera progresiva de un punto a otro de un proceso interno determinado o de un proceso a otro realizado por una unidad operativa dada. Se dividen en dos:

- ✓ Rastreo progresivo
- ✓ Rastreo regresivo

d) **Revisión Selectiva. -** Consiste en el examen ocular rápido de una parte de los datos o partidas que conforman un universo homogéneo en ciertas áreas, actividades o documentos elaborados.

5. Técnicas de Verificación Física

a) **Inspección. -** Es el examen físico y ocular de activos, obras, documentos y valores con el objetivo de establecer su existencia y autenticidad. La aplicación de esta técnica es de mucha utilidad, especialmente en cuanto a la constatación de efectivo, valores, activo físico y otros equivalentes.

2.2.5. EVIDENCIA DE AUDITORÍA

Según RC-273-2014-CG, es la información utilizada por el auditor para alcanzar las conclusiones en las que basa su opinión y sustenta el informe de auditoría.

- Suficiente: Medida cuantitativa, referida a la cantidad de evidencia obtenida.

- Apropiada: Medida cuantitativa, referida a la relevancia, fiabilidad y legalmente valida.

En función a la fuente empleada para su obtención la evidencia se clasifica de la siguiente manera:

- ✓ **Evidencia física:** Este tipo de evidencia se obtiene a través de una inspección u observación directa de las actividades, bienes o sucesos.

- ✓ **Evidencia documental:** Consiste en la información elaborada por la administración de la entidad relacionado con el desarrollo de su desempeño funcional; asimismo, la que establece las normas procesales pertinentes en caso de determinación de responsabilidades civiles y penales.

- ✓ **Evidencia testimonial:** Se obtiene de otras personas en forma de declaraciones hechas en el curso de las investigaciones o entrevistas.

- ✓ **Evidencia analítica:** Comprende análisis, conciliaciones, tabulaciones, cálculos y comparaciones de la información en sus componentes.

La evidencia es de naturaleza acumulativa y se obtiene principalmente de la aplicación de procedimientos de auditoria en el transcurso de la misma; no obstante, también puede incluir información obtenida de otras fuentes, como por ejemplo, auditorias anteriores, información preparada utilizando el trabajo de un experto, entre otras.

La evidencia de auditoria se consigue para verificar la legalidad, exactitud y consistencia de los registros de la entidad auditada.

2.2.6. COMISIÓN AUDITORA

Según la RC-070-2018-CG, la comisión auditora es el equipo multidisciplinario de auditores gubernamentales encargados de realizar la auditoria de cumplimiento derivada del control concurrente en el marco de las disposiciones y procedimientos técnicos establecidos por la Contraloría.

La comisión auditora debe disertar procedimientos de auditoria que permitan determinar de forma razonable el grado de cumplimiento normativo. En estos casos, el auditor debe asegurarse que la evidencia sea generada por medios que la ley admite, provenga de una fuente idónea y confiable, y que las copias

sean autenticadas con la firma de una autoridad de la entidad (fedatario o responsable de la unidad orgánica generadora del documento original)

Está conformada por un supervisor, un jefe de comisión e integrantes que incluyen obligatoriamente a un abogado y los profesionales que correspondan según la materia a examinar. Los roles del supervisor y jefe de la comisión para la auditoria de cumplimiento derivada del control concurrente, recae en los auditores que han ejercido dichos roles durante el desarrollo del control concurrente que motiva la ejecución del servicio de control posterior.

Excepcionalmente, por razones de desvinculación laboral, licencia u otras situaciones debidamente acreditadas y sustentadas la unidad orgánica que tiene a su cargo la auditoria de cumplimiento derivada del control concurrente con el visto bueno de la unidad orgánica de la cual depende, podrá designar a otros auditores en los roles de supervisor o jefe de la comisión auditora.

2.2.7. AMENAZAS Y VULNERABILIDADES

2.2.7.1. Amenazas

De acuerdo con la norma ISO 27000, citado por López, A.; (2011), se considera amenaza aquella causa potencial de un incidente no deseado, el cual puede causar daño a un sistema o a una organización. Alexander y otros (2007), coinciden en que las amenazas se pueden clasificar en grandes grupos para facilitar la toma de decisiones genéricas que reduzcan grupos de amenazas bajo una sola acción. Los grupos propuestos son:

- Naturales. Fuego, inundación, terremotos, etcétera.
- Humanas Accidentales. Desconocimiento, negligencia, despidos, pérdida no intencional de información.
- Humanas Intencionales. Robo de información, ataques.
- Tecnológicas. Virus, hacker, crackers, pérdida de datos, fallas de software, hardware o de red.

Luego de identificadas todas las amenazas, se evalúa su probabilidad de ocurrencia. El resultado de esta evaluación permitirá identificar las amenazas de mayor a menor concurrencia y la decisión sobre cuales atacar y cuales descartar de acuerdo con criterios técnicos, legales y de costos.

2.2.7.2. Vulnerabilidades

Según López, A.; (2011), las vulnerabilidades están asociadas a debilidades de los activos de información. La vulnerabilidad en el contexto de los sistemas de información es considerada como la ausencia o debilidad en los controles que ayudan a mitigar un riesgo, aumentando el nivel de impacto y el factor de exposición.

Las amenazas y las vulnerabilidades tienen interrelación, se parte de la pregunta sobre cuáles vulnerabilidades son aprovechadas por las amenazas, pues, una vulnerabilidad identificada genera amenazas que se convierten en un riesgo expuesto sobre cualquier sistema de información. Esto es lo que para expertos en temas de seguridad de información se conoce como la relación causa-efecto entre los elementos del análisis de riesgo. Por lo tanto, el siguiente paso será el de integrar

estos elementos para analizar y definir los niveles de riesgo que luego permitirán implementar los procedimientos que ayudarán a mitigar tales riesgos y eliminar las vulnerabilidades.

2.2.8. SISTEMAS DE INFORMACIÓN

De acuerdo a Cereni, M. & PRA, P.; (2012), un Sistema de Información (SI) es un conjunto de componentes interrelacionados para recolectar, manipular y diseminar datos e información y para disponer de un mecanismo de retroalimentación útil en el cumplimiento de un objetivo. Todos interactuamos en forma cotidiana con sistemas de información, para fines tanto personales como profesionales; utilizamos cajeros automáticos, los empleados de las tiendas registran nuestras compras sirviéndose de códigos de barras y escáner u obtenemos información en módulos equipados con pantallas sensibles al tacto, las muy famosas touchscreen. Las principales compañías gastan en la actualidad más de 1 000 millones de dólares al año en tecnología de información y el futuro dependeremos aún más de los sistemas de información.

Los sistemas de información contienen información acerca de gente, lugares y cosas importantes dentro de la organización o en el entorno que se desenvuelven. Por información se entiende los datos que se han modelado en una forma significativa y útil para los seres humanos. En contraste, los datos son consecuencia de los hechos en bruto y representan eventos que ocurren en las organizaciones o en el entorno físico antes de ser organizados y ordenados en una forma que las personas puedan entender y utilizar.

Hay tres actividades en un sistema de información que producen la información que las organizaciones necesitan para tomar decisiones, controlar operaciones, analizar problemas y creas

nuevos productos o servicios. Estas actividades son entrada, procesamiento y salida. La entrada captura o recolecta datos en bruto tanto al interior de la organización como de su entorno externo. El procesamiento convierte esta entrada de datos en una forma significativa. La salida transfiere la información procesada a la gente que lo usará o a las actividades para las que se utilizará. Los sistemas de información también requieren retroalimentación que es la salida que se devuelve al personal adecuado de la organización para ayudarle a evaluar o corregir la etapa de entrada.

2.2.9. LEY Nª 27785: LEY ORGANICA DEL SISTEMA NACIONAL DE CONTROL Y DE LA CONTRALORIA GENERAL DE LA REPUBLICA.

2.2.9.1. Ámbito de aplicación

Según el art. 3 de la ley 27785 Ley orgánica del sistema nacional de control y de la Contraloría General de la República, a la letra dice:

Las normas contenidas en la presente Ley y aquellas que emita la Contraloría General son aplicables a todas las entidades sujetas a control por el Sistema, independientemente del régimen legal o fuente de financiamiento bajo el cual operen. Dichas entidades sujetas a control por el Sistema, que en adelante se designan con el nombre genérico de entidades, son las siguientes:

- El Gobierno Central, sus entidades y órganos que, bajo cualquier denominación, formen parte del Poder Ejecutivo, incluyendo las Fuerzas Armadas y la Policía Nacional, y sus respectivas instituciones.

- Los Gobiernos Regionales y Locales e instituciones y empresas pertenecientes a los mismos, por los recursos y bienes materia de su participación accionaria.
- Las unidades administrativas del Poder Legislativo, del Poder Judicial y del Ministerio Público.
- Los Organismos Autónomos creados por la Constitución Política del Estado y por ley, e instituciones y personas de derecho público.
- Los organismos reguladores de los servicios públicos y las entidades a cargo de supervisar el cumplimiento de los compromisos de inversión provenientes de contratos de privatización.
- Las empresas del Estado, así como aquellas empresas en las que éste participe en el accionariado, cualquiera sea la forma societaria que adopten, por los recursos y bienes materia de dicha participación.
- Las entidades privadas, las entidades no gubernamentales y las entidades internacionales, exclusivamente por los recursos y bienes del Estado que perciban o administren. En estos casos, la entidad sujeta a control, deberá prever los mecanismos necesarios que permitan el control detallado por parte del Sistema.

2.2.9.2. Control interno

Artículo 7: El control interno comprende las acciones de cautela previa, simultánea y de verificación posterior que realiza la entidad sujeta a control, con la finalidad que la gestión de sus recursos, bienes y operaciones se efectúe correcta y eficientemente. Su ejercicio es previo, simultáneo y posterior. El control interno previo y simultáneo compete exclusivamente a las autoridades, funcionarios y servidores públicos de las entidades como

responsabilidad propia de las funciones que le son inherentes, sobre la base delas normas que rigen las actividades de la organización y los procedimientos establecidos en sus planes, reglamentos, manuales y disposiciones institucionales, los que contienen las políticas y métodos de autorización, registro, verificación, evaluación, seguridad y protección. El control interno posterior es ejercido por los responsables superiores del servidor o funcionario ejecutor, en función del cumplimiento de las disposiciones establecidas, así como por el órgano de control institucional según sus planes y programas anuales, evaluando y verificando los aspectos administrativos del uso de los recursos y bienes del Estado, así como la gestión y ejecución llevadas a cabo, en relación con las metas trazadas y resultados obtenidos.

2.2.9.3. Control externo

Artículo 8: Se entiende por control externo el conjunto de políticas, normas, métodos y procedimientos técnicos, que compete aplicar a la Contraloría General u otro órgano del Sistema por encargo o designación de ésta, con el objeto de supervisar, vigilar y verificar la gestión, la captación y el uso de los recursos y bienes del Estado. Se realiza fundamentalmente mediante acciones de control con carácter selectivo y posterior.

2.2.9.4. Acción de control

Artículo 10: La acción de control es la herramienta esencial del Sistema, por la cual el personal técnico de sus órganos conformantes, mediante la aplicación de las normas, procedimientos y principios que regulan el control

gubernamental, efectúa la verificación y evaluación, objetiva y sistemática, de los actos y resultados producidos por la entidad en la gestión y ejecución de los recursos, bienes y operaciones institucionales.

2.2.9.5. **Sistema Nacional de Control**

Artículo 12: Es el conjunto de órganos de control, normas, métodos y procedimientos, estructurados e integrados funcionalmente, destinados a conducir y desarrollar el ejercicio del control gubernamental en forma descentralizada. Su actuación comprende todas las actividades y acciones en los campos administrativo, presupuestal, operativo y financiero de las entidades y alcanza al personal que presta servicios en ellas, independientemente del régimen que las regule.

2.2.9.6. **Conformación del Sistema Nacional de Control (SNC)**

Artículo 13: Conforman el SNC

a. La Contraloría General
b. Todas las unidades orgánicas responsables de la función de control gubernamental de las entidades que se mencionan en el Artículo 3º de la presente Ley,
c. Las sociedades de auditoría externa independientes, designadas por la Contraloría General y contratadas, durante un período determinado, para realizar servicios de auditoría económica, financiera, de sistemas informáticos, de medio ambiente y otros.

2.3. GLOSARIO DE TÉRMINOS

Aseguramiento Razonable – Según COBIT 4.1, es un estándar para la evaluación de la suficiencia de los procedimientos establecidos para cumplir con un objetivo de control en particular. El aseguramiento razonable involucra la aplicación del criterio, conocimiento y experiencia para desarrollar una opinión informada. El aseguramiento razonable requiere que un sistema de controles sea eficaz, pero no demasiado gravoso. El estándar de aseguramiento razonable también requiere que un sistema de controles sea eficiente en costos.

Controles Compensatorios – Según COBIT 4.1, son los pasos o procedimientos adicionales de control que no se relacionan directamente con el objetivo de control que se está probando, pero cuya presencia sirve para fortalecer los controles que sí se relacionan directamente con el objetivo de control. Los controles compensatorios se identifican durante la fase de pruebas de cumplimiento del trabajo de auditoría. Los controles compensatorios se procuran de manera activa solamente cuando la eficacia de los controles establecidos es cuestionable.

Criterio de auditoría: Según Directiva N° 007-2014-CG/GCSII, norma o disposición aplicable a la materia a examinar.

Documentación de auditoría: Según Directiva N° 007-2014-CG/GCSII, es la evidencia documental del trabajo del auditor y está constituida por el plan de auditoría y su sustento, la evidencia obtenida como resultado de la aplicación de los procedimientos de auditoría, la documentación generada por la comisión auditora que contiene el análisis y conclusiones respecto a la evidencia obtenida, así como los informes de auditoría emitidos. Esta documentación debe estar clasificada y referenciada en los archivos de auditoría, constituidos por una o más carpetas u otros medios de almacenamiento de datos, físicos o electrónicos; facilitando su accesibilidad,

uso y custodia correspondiente, en beneficio de la celeridad y seguridad de las actividades que forman parte de la auditoría.

Muestreo de auditoría: Según Directiva N° 007-2014-CG/GCSII, es la aplicación de los procedimientos de auditoría a un porcentaje inferior al 100% de los elementos de una población relevante para la auditoría, de forma que todas las unidades de muestreo tengan posibilidad de ser seleccionadas con el fi n de proporcionar al auditor una base razonable a partir de la cual alcanzar conclusiones sobre toda la población.

Juicio profesional: Según Directiva N° 007-2014-CG/GCSII, Aplicación de la formación práctica, el conocimiento y la experiencia relevantes, en el contexto de las normas de auditoría, contabilidad y ética, para la toma de decisiones acerca del curso de acción adecuado, en función de las circunstancias del encargo de auditoría.

Objetivo de Control: Según COBIT 4.1, es una definición del resultado o propósito que se desea alcanzar implementando procedimientos de control específicos dentro de una actividad de tecnología informática y sistemas de información.

Plan de auditoría: Según Directiva N° 007-2014-CG/GCSII, es un documento que resume las decisiones más importantes relativas a la estrategia para el desarrollo de la auditoría de cumplimiento. Determina entre otros aspectos, los objetivos y alcance de la auditoría, la materia a examinar y los recursos para su ejecución. Incluye el programa con procedimientos de auditoría.

Procedimientos Reales – Según COBIT 4.1, son los procedimientos que están siendo realizados por la organización para satisfacer el objetivo de auditoría. Los procedimientos reales se identifican durante la fase de auditoría de pruebas de cumplimiento.

Procedimiento de auditoria: Según Directiva N° 007-2014-CG/GCSII, son el conjunto de técnicas de investigación necesarias para efectuar el examen o revisión de una partida, hecho o circunstancia. Un procedimiento de auditoria es la aplicación de una o varias técnicas de auditoria para obtener evidencias de auditoria.

Programa de auditoría: Según Directiva N° 007-2014-CG/GCSII, documento, donde se señalan los objetivos y procedimientos que deben ser ejecutados por la comisión auditora.

Recomendación: Según Directiva N° 007-2014-CG/GCSII, Medida específica de factibilidad técnica, económica y legal, que con el propósito de mostrar los beneficios que reportará la auditoría de cumplimiento, se recomiendan a la administración de la entidad para promover mejoras y superar las causas y desviaciones de cumplimiento, debiéndose ejecutar en un plazo perentorio en salvaguarda de los bienes y recursos públicos, y de la función pública.

Riesgo: Según RC N° 273-2014-CG, posibilidad que ocurra un evento adverso que afecte el logro de los objetivos de una entidad. Se expresa en términos de probabilidad e impacto.

Riesgo de auditoría: Según RC N° 273-2014-CG, Se refiere a que el informe de auditoría - o más específicamente la conclusión o dictamen del auditor - no sea el apropiado a las circunstancias de la auditoría.

Sociedades de auditoría: De acuerdo al artículo 17 de la ley 27785, son personas jurídicas calificadas e independientes en la realización de labores de control posterior externo, designadas por la Contraloría General, previo Concurso Público de Méritos, y contratadas por las entidades para examinar las actividades y operaciones de las mismas, opinar sobre la razonabilidad de sus estados financieros, así como evaluar la gestión, captación y uso de los recursos asignados.

Técnica de auditoría: Según Directiva N° 007-2014-CG/GCSII, son los métodos prácticos de investigación y prueba que el auditor utiliza para obtener la evidencia necesaria que le permita fundamentar su opinión profesional. Su empleo se basa en el criterio o juicio profesional, según las circunstancias.

Unidades Orgánicas: De acuerdo al artículo 17 de la ley 27785, son los órganos de auditoría interna de las entidades comprendidas en los incisos a), b), c) y d) del Artículo 3º de la presente Ley, así como las empresas en las que el Estado tenga una participación accionaria total o mayoritaria, tendrán necesariamente un Órgano de Auditoría Interna ubicado en el mayor nivel jerárquico de la estructura de la entidad, el cual constituye la unidad especializada responsable de llevar a cabo el control gubernamental en la entidad.

2.4. MARCO INSTITUCIONAL GUBERNAMENTAL

2.4.1. ORGANIZACIÓN DEL ESTADO PERUANO

Según IDEA internacional (2008) citado por SERVIR (2016), La división de poderes en el Estado Peruano es de dos tipos: horizontal en el que se establecen tres poderes que se controlan entre sí (Legislativo, Ejecutivo y Judicial); y, vertical en donde el poder se redistribuye en tres niveles de gobierno (Central, Regional y Municipal).

2.4.1.1. Poder Ejecutivo

Según IDEA internacional (2008) citado por SERVIR (2016), el Poder Ejecutivo está conformado por la

Presidencia de la República, el Consejo de Ministros, Ministerios, Organismos Públicos Descentralizados, proyectos, programas, empresas de propiedad del gobierno nacional

Los Organismos Públicos

De conformidad con la Ley Orgánica del Poder Ejecutivo - Ley 29158, los organismos públicos son entidades desconcentradas del Poder Ejecutivo, con personería jurídica de Derecho Público y tienen competencias de alcance nacional. Estos organismos están adscritos a un Ministerio y para su creación y disolución se debe hacer por Ley a iniciativa del Poder Ejecutivo. Pueden ser de dos tipos:

Organismos Públicos Ejecutores.
Organismos Públicos Especializados.

En ambos casos, su reorganización, fusión, cambio de dependencia o adscripción se debe acordar por voto aprobatorio del Consejo de Ministros. Existen actualmente 60 organismos públicos.

En el caso de los Organismos Públicos Ejecutores, éstos se crean cuando existen condiciones como la necesidad de contar con una entidad con administración propia debido a la magnitud de las operaciones o para la prestación de servicios específicos. Actualmente existen 41 Organismos Ejecutores entre los que destacan el Consejo Nacional de Ciencia Y Tecnología (CONCITEC), Instituto Nacional Penitenciario (INPE), Superintendencia Nacional de Administración Tributaria (SUNAT).

Los Organismos Públicos Especializados están adscritos a un Ministerio y pueden ser de dos tipos: i) Organismos Reguladores; y, ii) Organismos Técnicos Especializados.

Existen cuatro Organismos Reguladores: OSITRAN, OSINERGMIN, OSIPTEL y SUNASS.

Actualmente se cuenta con 15 organismos especializados dentro de los cuales destaca el Organismos de Evaluación y Fiscalización Ambiental (OEFA) recientemente creado adscrito al Ministerio del Ambiente; el Centro de Planeamiento Estratégico - CEPLAN y la Autoridad Nacional de v Servicio Civil

Programas y proyectos especiales

Los Programas son estructuras funcionales creadas para atender un problema o situación crítica, o implementar una política pública específica, en el ámbito de competencia de la entidad a la que pertenecen.

Los Proyectos Especiales son un conjunto articulado y coherente de actividades orientadas a alcanzar uno o varios objetivos en un período limitado de tiempo, siguiendo una metodología definida.

Las empresas públicas

En el Perú, la actividad empresarial está -en principio- reservada para el sector privado. Ocurre, sin embargo, que no siempre el sector privado está en capacidad de brindar determinados servicios u ofrecer ciertos bienes considerados de interés público. Sólo en ese supuesto, y autorizado por ley expresa, el Estado participa en el mercado de manera subsidiaria.

Fig. 01: Estructura del Poder Ejecutivo

2.4.1.2. Poder Legislativo

Según IDEA internacional (2008), citado por SERVIR (2016), La estructura del Parlamento se puede dividir en su ámbito político y administrativo, tal y como se muestra en el siguiente diagrama.

Fig. 02: Estructura del Poder Legislativo

Ámbito Administrativo

En su ámbito administrativo, el Congreso cumple un rol técnico, imparcial y no partidario. Su máximo órgano es

la Oficialía Mayor que ejecuta diversas funciones tales como: la preparación de la agenda del pleno, de la Comisión Permanente y del Consejo Directivo; organizar y dirigir el servicio parlamentario, entre otras.

2.4.1.3. Organismos Autónomos

La Constitución de la República establece órganos autónomos que no son parte de ningún poder del Estado, cuyos titulares responden directamente ante el Congreso y a la opinión pública. En la mayor parte de estos organismos, los procedimientos de designación contemplan la intervención del Poder Ejecutivo, Legislativo y, en algunos casos, el Poder Judicial. Una vez designado, los titulares o directores son inamovibles por períodos de tiempo o condiciones (edad) predeterminadas. Así son órganos constitucionalmente autónomos el Banco Central de la Reserva, Superintendencia de Banca y Seguros, Tribunal Constitucional, Ministerio Público, Consejo Nacional de la Magistratura, Defensor del Pueblo, Sistema Electoral (Jurado Nacional de Elecciones, Oficina Nacional de Procesos Electorales y Registro de Identificación) y Contraloría General de la República.

2.4.1.4. Gobiernos Regionales y Locales

El Perú cuenta con 24 Departamentos o circunscripciones político administrativas, gobernados por 26 gobiernos regionales (Lima cuenta con dos Gobiernos Regionales, Lima Metropolitana y Lima Provincias, y la Provincia Constitucional del Callao cuenta con un Gobierno Regional propio). Los Departamentos están conformados por 195 provincias y éstas, a su vez, por 1.634 distritos.

El Gobierno Regional es ejercido por el Presidente Regional, de acuerdo a las competencias, atribuciones y funciones que le asigna la Constitución, la Ley de Bases de Descentralización y la Ley Orgánica de Gobiernos Regionales. Cuentan con autonomía política, económica y administrativa en los asuntos de su competencia.

El Alcalde es el representante legal de la Municipalidad y su máxima autoridad administrativa. Los Gobiernos Locales cuentan con el mismo nivel de autonomía que el de las Regiones de acuerdo a la Ley Orgánica de Municipalidades.

2.5. HIPÓTESIS

La Propuesta de un modelo de auditoría de sistemas de Información podrá ser utilizado en las acciones de control en una auditoría de TIC para una entidad pública.

2.5.1. VARIABLES

2.5.1.1. Variable de investigación

Modelo de auditoria de sistemas de información.

Tabla 01: Operacionalización de Variables

VARIABLE	DEFINICION CONCEPTUAL	INDICADOR
Modelo de auditoria de sistemas de información	Es un referente para elaborar implementar acciones de control y procedimientos de auditoría relacionados a sistemas de información. Es una herramienta para efectuar la verificación y evaluación, objetiva y sistemática de los sistemas de información.	Plan de auditoría
		Programa de auditoría.
		Objetivos de control
		Actividades en los procedimientos de auditoria
		Técnicas utilizadas en los procedimientos de auditoria.
		Pruebas utilizadas en los procedimientos de auditoria.

CAPÍTULO III
MARCO METODOLÓGICO

3.1. ENFOQUE Y DISEÑO

3.1.1. ENFOQUE DE LA INVESTIGACIÓN

El presente trabajo de investigación es de tipo **APLICADA FUNDAMENTAL** con un enfoque **CUANTITATIVO**.

3.1.2. DISEÑO DE LA INVESTIGACIÓN

En la presente investigación sigue un diseño NO EXPERIMENTAL, no existe manipulación de las variables. El alcance tiene un nivel **DESCRIPTIVO,** debido a que mide las diferentes variables o conceptos, describiendo situaciones.

3.2. SUJETOS DE LA INVESTIGACIÓN

Los sujetos de la investigación son las entidades del sector público comprendidas en el marco de la ley 27785, El criterio de inclusión y exclusión considerado para la delimitación poblacional son los sistemas de información que operan en las entidades públicas del país. Como la población es muy grande se tomó una muestra de dos entidades públicas de la región Piura a discreción del investigador, para evaluar los controles y auditar los sistemas de información que operan en las principales entidades gubernamentales del país.

3.3. MÉTODOS Y PROCEDIMIENTOS

Para medir y recolectar la información necesaria se va a evaluar los sistemas de información que existen en algunas entidades públicas de la región y se contrastarán con los documentos técnicos y normativos existentes y vigentes aplicables.

3.4. TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE DATOS

2.1.1. TÉCNICAS

Las técnicas de recolección de datos, consiste en recolectar datos de fuentes primarias. Para la presente investigación utilizaremos:

Observación Estructurada

Sierra y Bravo (1984), definen la observación como la inspección y estudio realizado por el investigador mediante el empleo de sus propios sentidos, con o sin ayuda de aparatos técnicas, de las cosas o hechos de interés social, tal como son o tienen lugar espontáneamente.

2.1.2. INSTRUMENTOS

La observación estructurada se realizará con la ayuda de fichas de observación.

CAPÍTULO IV
RESULTADOS Y DISCUSIÓN

4.1. PROPUESTA DEL MODELO DE AUDITORÍA DE SISTEMAS DE INFORMACIÓN PARA ENTIDADES PÚBLICAS.

Para elaborar el modelo, se tomó como marco de referencia el cuerpo normativo vigente del Estado Peruano, la NTP 17799, modelos internacionales de auditoría existentes como COBIT y la ISO 27001. De acuerdo a lo dispuesto por la Contraloría General de la República del Perú, la auditoría en el sector público sigue tres fases: la planificación, la ejecución y el informe final, también podemos mencionar una fase adicional que es el seguimiento.

Tomando como referencia lo señalado en el párrafo anterior se elaboró el modelo de auditoría de sistemas de información propuesto que a continuación describo:

4.1.1. FASE DE PLANIFICACIÓN

En esta fase se debe seguir el siguiente procedimiento: Primero, el auditor de sistemas convoca a una serie de reuniones con los interesados de la realización de la auditoría en la entidad pública, el auditor delimita el alcance de la auditoría, los objetivos de la misma, el tipo de auditoría informática que se va a practicar, que puede ser sobre:

- ✓ Desarrollo integral de auditoria de sistemas de información.
- ✓ Auditoria exclusiva de algún sistema o subsistema de información específico.
- ✓ Auditoria de alguna función en particular como: la seguridad y privacidad.
- ✓ Auditoria sobre la metodología de desarrollo del sistema de información.
- ✓ Auditoría sobre la base de datos del sistema de información.
- ✓ Auditoría sobre el costo real del sistema de información.

- ✓ Auditoría sobre el performance del sistema de información

Segundo, el auditor debe tener una comprensión global de la institución, para lo cual utiliza una serie de acciones como revisión de documentos de gestión y normativos de la entidad pública, puede realizar muestreos no probabilísticos de carácter selectivo sobre los procesos o las tareas para obtener una idea de la dimensión y complejidad del ámbito de estudio, lo que permitirá estimar esfuerzos.

Tercero, el auditor debe determinar los perfiles de los profesionales que conformarán el equipo de auditoría de sistemas de información, los especialistas deben ser elegidos tomando como referencia los tipos de auditoría señalados anteriormente. Entre los perfiles propuestos tenemos:

- ✓ Especialista en comunicación de datos y redes
- ✓ Especialista en base de datos
- ✓ Especialista en configuración de hardware y software.
- ✓ Especialista en organización y realización del trabajo administrativo
- ✓ Especialista en proyectos de desarrollo de sistemas de información
- ✓ Especialista en metodologías de desarrollo de software
- ✓ Especialista en lenguajes de programación
- ✓ Especialista en centros de procesamiento de datos
- ✓ Especialista en costeo de software y hardware

Cuarto, el auditor debe determinar los recursos materiales mínimos necesarios, para llevar a cabo la auditoría sin limitaciones, para alcanzar el cumplimiento de cada uno de los objetivos de control. Entre los recursos tenemos:

- ✓ Lenguajes de programación
- ✓ Sistemas de administración de bases de datos
- ✓ Equipos de cómputo específicos
- ✓ Internet

Quinto, el producto final de la fase, es elaborar un Plan de Auditoría de Sistemas (Formato Nº 01) y un Programa de Auditoría de Sistemas (Formato Nº 02) de acuerdo a la siguiente estructura:

Formato Nº 01

PLAN DE AUDITORÍA DE SISTEMAS

I. Origen y Tipo de la Auditoría
II. Comprensión General de la Entidad
III. Procesos, tareas y/o temas a evaluar
IV. Objetivos, criterios, alcance y periodo de la auditoría
    4.1. Objetivo General
    4.2 Objetivos Específicos
    4.3 Criterios de la auditoría
    4.4 Alcance de la auditoría
    4.5 Periodo a examinar
V. Especialistas que participan en la auditoría

PERSONAL NECESARIO

NOMBRES Y APELLIDOS	PROFESION	CARGO

Elaboración propia

VI. Administración de recursos
    6.1. Presupuesto de tiempo

Tiempo estimado por etapas

ACTIVIDADES	DIAS UTILES	TOTAL PERSONAS	DIAS CALENDARIO	
			DEL	AL
PLANIFICACION				
EJECUCIÓN				
COMUNICACIÓN DE DEFICIENCIAS O FALLAS				
EVALUACION DE DESCARGOS				
REDACCION DE INFORME				
SUPERVISION, SUSTENTO Y ELEVACION DE INFORME				
TOTAL DIAS UTILES				

Elaboración propia

Horas Hombre Programadas

CARGO	PLANIFICACIÓN	EJECUCIÓN	COMUNICACIÓN DE DEFICIENCIAS	EVALUACIÓN DE DESCARGOS	REDACCIÓN DEL INFORME	SUPERVISIÓN SUSTENTACIÓN Y ELEVACIÓN DE INFORME	TOTAL HORAS HOMBRE
Supervisor							
Auditor							
Especialista 1							
Especialista 2							
Especialista n							
TOTALES							

6.2. Costo de la auditoría

6.3. Fecha de entrega del informe de auditoría

6.4. Formato propuesto del informe de auditoría

Formato Nº 02

PROGRAMA DETALLADO DE AUDITORÍA DE SISTEMAS

Nombre de la Entidad: **.....**

Fecha de auditoría: .....

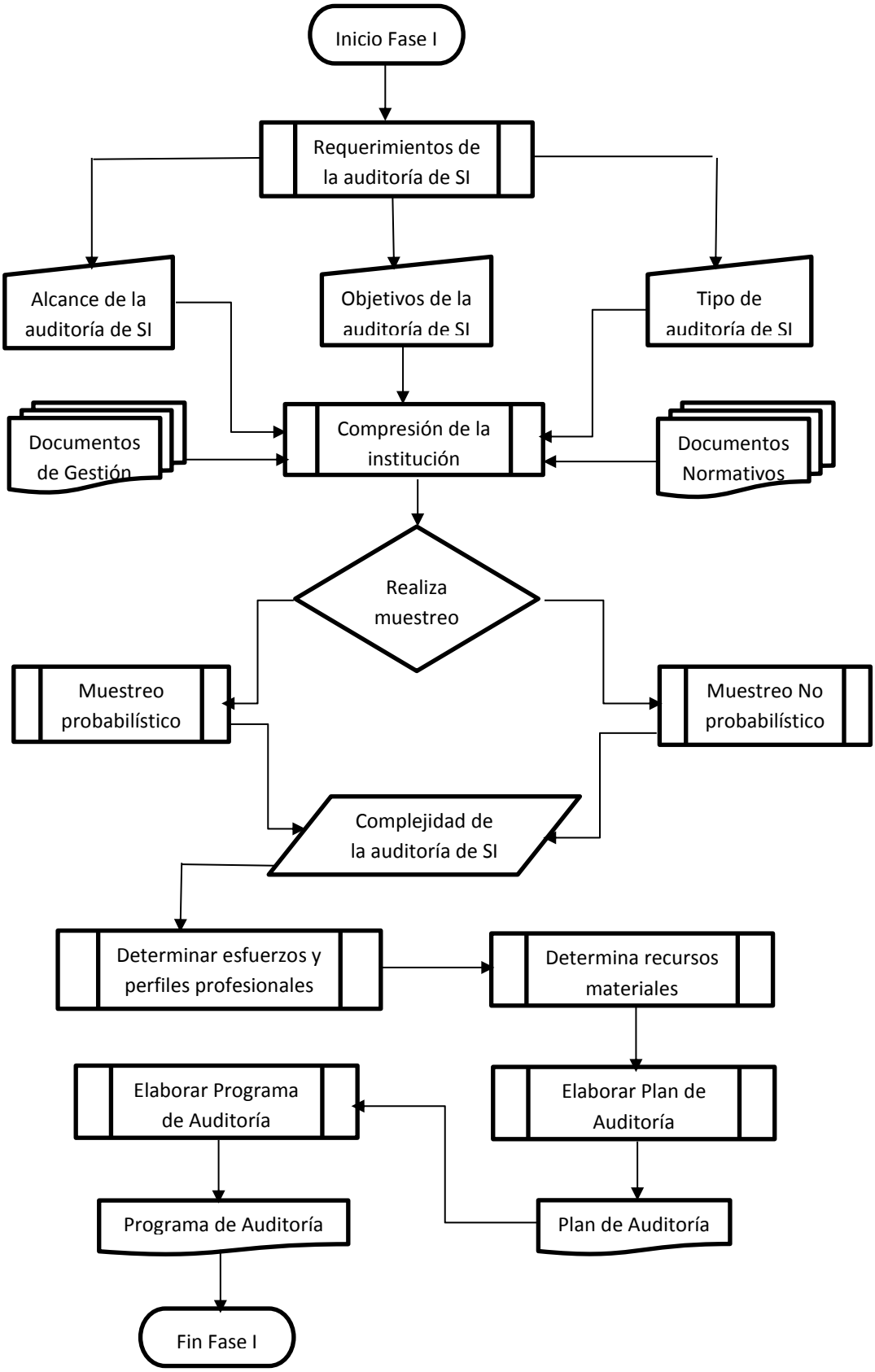
PROCEDIMIENTOS	REF. P/T	HECHO POR	FECHA PROGRAMADA	FECHA EJECUCIÓN	HORAS TOTALES
OBJETIVO DE CONTROL **Procedimientos de auditoría** Procedimiento 1 Procedimiento 2 … Procedimiento n **Criterios de auditoría** Criterio 1 Criterio 2 … Criterio n					

Revisado por (Encargado/Supervisor)_____Fecha_____

Aprobado por (Auditor) _____Fecha_____

Gráfico Nº 01

FLUJOGRAMA PROPUESTO: FASE I DE PLANIFICACIÓN



Fuente: Elaboración Propia

Como parte del modelo de auditoría propuesto, se proponen objetivos de control para realizar auditorías en algunas áreas de los sistemas de información, de acuerdo a la necesidad requerida por la entidad pública que solicita la auditoría de sistemas.

Objetivos de control para la organización del área de la oficina de sistemas

- Verificar que el manual de organización y funciones de la entidad considere la segregación de funciones en el personal del área de informática.

- Comprobar la eficiencia del área de informática y que sus recursos sean administrados de forma apropiada.

- Verificar una buena planificación, organización, control, estandarización, etc., dentro del área; que todos los proyectos sean abordados por medio de un estudio de factibilidad previo, y que no se decidan por la MODA que impera en el mercado o que traten de imponer proveedores de software y hardware.

- Verificar la eficiencia dentro del área de informática, ya que se trata de un área costosa, debido a factores tales como:
  - ✓ Tecnología costosa
  - ✓ Especialistas escasos y de altas remuneraciones.
  - ✓ Cambios tecnológicos y rápidos.
  - ✓ Obsolescencia de los sistemas en corto plazo (3 años máx.)
  - ✓ Insumos de alto costo.
  - ✓ Desarrollo lento de sistemas de información.

- Verificar que la entidad cuenta con un Comité de Usuarios de Sistemas de Información integrado por representantes de las diferentes áreas, además posee un Comité Directivo. Estos comités elaboran y controlan el Plan de Sistemas de Información (PSI).

Objetivos de control para evaluar base de datos, archivos y datos

- Corroborar la existencia de controles de seguridad en las bases de datos para proteger la información almacenada, contra su pérdida o robo, la cual es uno de los principales activos para la entidad.

- Verificar la existencia de controles para proteger los datos contra accesos no autorizados y así evitar la alteración o destrucción maliciosa de los mismos por parte de individuos, sea accidental o de forma intencional.

- Identificar los controles de seguridad utilizados para mantener la integridad de los datos y la base de datos.

- Verificar los controles para la realización de backups de las bases de datos y de los archivos que contienen información sensible y crítica para la entidad, como medida para prevenir posibles fallos.

- Verificar si existe inconsistencia de los datos en la base de datos para evitar al mínimo la redundancia y preservando en todo momento la integridad de los datos.

Objetivos de control para evaluar el plan de capacitación para utilizar los sistemas de información

- Comprobar si la Entidad cuenta con un presupuesto anual para capacitación.

- Investigar si existe un plan de la capacitación y de desarrollo profesional de los miembros del personal de TI y/o de los usuarios del software.

- Comprobar si el contenido de los cursos cuenta con un nivel de detalle, acorde con las necesidades de los usuarios.

- Comprobar si la Entidad cuenta con un proceso de Administración del conocimiento por persona.

- Revisar la documentación que tiene el área de soporte (sistemas), e identificar el inventario de problemas, donde la causa raíz sea la capacitación.

Objetivos de control sobre seguridad física y lógica

- Identificar si el software instalado en los equipos cuenta con licencias adquiridas por la organización.

- Realizar una revisión exhaustiva en la entidad para identificar equipos con antivirus instalados y actualizados.

- Realizar una evaluación de las cuentas activas y el usuario asignado para cada una de ellas.

- Identificar que todos los usuarios asignados a los trabajadores cesados estén respectivamente desactivados.

- Identificar la actualización de parches de seguridad en los servidores de la empresa.

- Verificar la existencia de controles sobre el acceso físico a las instalaciones, la seguridad física de las mismas, equipos, programas y medios de almacenamiento del área de informática.

Objetivos de control para evaluar el desarrollo y mantenimiento de sistemas de información

- Verificar si antes de desarrollar un sistema de información se hacen estudios formales de factibilidad y costos.

- Confirmar la eficiencia, eficacia y confiabilidad de los sistemas de información en la etapa de producción (explotación), mediante la implementación de procedimientos que garanticen su adecuada operatividad.

- Comprobar que los procedimientos de desarrollo y mantenimiento incluyen pistas de auditoría y control en los sistemas.

- Verificar que el área de informática cumpla con los plazos estipulados en el desarrollo de los sistemas, para garantizar buenos resultados, ya que entregar información correcta y oportuna es fundamental para la toma de decisiones.

- Verificar si existe la documentación durante el desarrollo de los sistemas de información.

4.1.2. FASE DE EJECUCIÓN

Después de contar con el Plan de auditoría de SI y Programa de auditoría de SI, se inicia la fase de ejecución, donde el especialista en auditoría de SI de acuerdo a su perfil procederá a la aplicación de los procedimientos de auditoría, del objetivo de control que le corresponda de acuerdo a lo especificado en el programa de auditoría. A continuación, desarrollamos los pasos que debe realizar el especialista en esta fase.

Primero, localización del objeto o hecho auditable, y, la identificación de las personas que están relacionadas con el objeto o el hecho,

también identificamos la normativa que la institución o área auditada puede tener en relación al objeto o hecho.

Como resultado, el auditor o especialista de SI deberá haber identificado, documentado y verificado:

- ✓ Quién realiza la tarea y/o actividad cubierta por el objetivo de control
- ✓ Dónde se realiza la tarea y/o actividad
- ✓ Cuándo se realiza la tarea y/o actividad
- ✓ Sobre qué datos de entrada se realiza la tarea y/o actividad
- ✓ Qué datos de salida/resultados se esperan de la tarea y/o actividad, y
- ✓ Cuáles son los procedimientos establecidos por la institución para realizar la tarea y/o actividad.

Segundo, evaluación de procedimientos establecidos por la institución para realizar la tarea y/o actividad materia de auditoría, para verificar si el control que ejercen dichos procedimientos es eficaz. Los procedimientos deben evaluarse contra la normativa prevista, las prácticas estándar del sector público y el criterio del auditor. Lo que se pretende es verificar que se está cumpliendo el objetivo de control.

Como resultado, el auditor o especialista debe haber:

- ✓ Evaluado la normativa de la entidad en cuanto a su aplicación sobre los procedimientos establecidos
- ✓ Evaluado los procedimientos establecidos para determinar si son eficientes en costos y proporcionan aseguramiento razonable de que se está realizando la tarea y de que se está cumpliendo el objetivo de control

Tercero, deberá realizarse entrevistas y revisión de documentos para determinar si los controles están debida y consistentemente aplicados. De ser así, se realizan las pruebas de cumplimiento.

Como resultado, el auditor debe haber documentado en sus papeles de trabajo (Formato Nº 03) los hallazgos o deficiencias, si los procedimientos establecidos están o no, debida y consistentemente aplicados.

Finalmente, el auditor de sistemas debe organizar toda la información que se obtiene en esta fase mediante un registro completo y detallado de la labor efectuada y las conclusiones alcanzadas, todo debe quedar registrado en los documentos denominados papeles de trabajo, donde cada especialista debe dejar constancia de las evidencias, así como de los procedimientos y técnicas de auditoría utilizados para recogerlas, del mismo modo las pruebas generales y específicas que se usaron. Los papeles de trabajo constituyen el vínculo entre la fase de planeamiento y la fase de ejecución de la auditoría, permiten una adecuada ejecución, revisión y supervisión del trabajo de auditoría. Con la evidencia que consta en los papeles de trabajo, el auditor fundamenta sus opiniones y conclusiones sobre los hallazgos o deficiencias encontradas sobre los asuntos auditados, opiniones y conclusiones que se presenten en el informe. Las evidencias pueden constar en medios de almacenamiento magnético, electrónicos, informáticos y otros. La estructura propuesta de los papeles de trabajo es la siguiente:

Formato Nº 03

PAPEL DE TRABAJO

AUDITORÍA DE SISTEMAS

Unidad Administrativa:
Elaborado por:
Referencia:
Revisó:
Cédula:

Objetivo de Control:

Procedimiento(s):

Observaciones:
Situación Real:

Técnicas de auditoría

Pruebas de auditoría

Situación Prevista:

Conclusiones:

Recomendaciones:

Elaborado por:	**Supervisado por:**
Fecha: xx de xx de xxxx	**Fecha: xx de xx de xxxx**

4.1.3. FASE DE INFORME DE AUDITORÍA

El resultado del trabajo realizado en la fase de ejecución de la auditoría es la elaboración del informe de auditoría por parte del auditor de sistemas, mediante este documento se expone el resultado del trabajo final, es decir, después de haber evaluado lo encontrado por los especialistas, lo cual ha sido plasmado en sus papeles de trabajo. Los hallazgos o deficiencias encontradas son comunicados por el auditor de sistemas a los involucrados, quienes luego hacen sus

descargos. Finalmente, estos descargos son evaluados nuevamente por el auditor, lo cual queda resuelto para plasmar en el informe final de auditoría. Como resultado de esta fase se proponen las características y estructuras que debe tener dicho informe (Formato Nº 04). Es aquí donde el auditor a través de juicios fundamentados en las evidencias obtenidas durante la fase de ejecución, brinda suficiente información a los funcionarios de la entidad pública auditada y estamentos pertinentes, sobre las deficiencias o desviaciones más significativas, e incluir las recomendaciones que permitan promover mejoras en la conducción de las actividades u operaciones del área o áreas examinadas.

La comisión auditora deberá adecuarse a los plazos estipulados en el programa de auditoría correspondiente, a fin que el informe pueda emitirse en el tiempo previsto, permitiendo que la información en él revelada sea utilizada oportunamente por el titular de la entidad y/o autoridades de los niveles apropiados del Estado.
En tal sentido, la Comisión Auditora debe prever que la elaboración del informe concluya en el plazo otorgado, a fin de permitir su emisión oportuna.

- ✓ El informe emitido debe cumplir con las siguientes características: calidad,
- ✓ confiabilidad,
- ✓ redacción mediante un lenguaje sencillo haciendo una crítica constructiva,
- ✓ concisión,
- ✓ exactitud coherente con los papeles de trabajo,
- ✓ orden,
- ✓ sistemático y
- ✓ objetivo al exponer los hechos.

Formato Nº 04

INFORME DE AUDITORÍA DE SISTEMAS

PROCESOS, TAREAS Y/O TEMAS DE LA AUDITORÍA DE SISTEMAS

1. Índice
2. Presentación
3. Definición, objetivos y ámbito
4. Enumeración de temas
5. Análisis
6. Conclusiones
7. Recomendaciones

4.2. APLICACIÓN DEL MODELO DE AUDITORÍA PROPUESTO

Para realizar una aplicación del modelo propuesto se tomó como referencia los objetivos de control relacionados con la capacitación del personal de TI, el modelo propuesto se ha ejecutado en la oficina de SUNARP (Superintendencia Nacional de Registros Públicos) de la ciudad de Otuzco – La Libertad. Es importante señalar que se han desarrollado las fases de auditoría de planificación y ejecución, que es donde el modelo propuesto brinda un mayor aporte.

4.2.1. FASE DE PLANIFICACIÓN – PLAN DE AUDITORÍA DE SISTEMAS DE INFORMACIÓN

Para el desarrollo de esta fase se siguieron los pasos propuestos por el modelo, pero al mismo tiempo el resultado de la aplicación de los pasos del modelo se plasma es el desarrollo del formato de Plan de Auditoría propuesto, lo mismo ocurre para el Programa de Auditoría.

PLAN DE AUDITORÍA DE SISTEMAS
"AUDITORÍA AL PROCESO DE CAPACITACION DEL PERSONAL EN EL USO DE LOS SISTEMAS DE INFORMACIÓN"

I. Origen y Tipo de la Auditoría

Este examen se efectúa en cumplimiento de las acciones de control programadas en el Plan Anual de Control 2018 de la Oficina de SUNARP de la ciudad de Otuzco – La Libertad.

II. Comprensión General de la Entidad

Las tecnologías de la información (TI) tienen mucho que aportar en los procesos de la Oficina de SUNARP – Otuzco a la cual en adelante llamaremos Oficina, al punto que no se puede pensar en ninguno de estos sin la participación de ellas. Decir que las TI son esenciales para mejorar la productividad de la Oficina, es algo que queda muy claro a la luz de la experiencia, pero el solo hecho de introducir tecnología en los procesos de la Oficina no garantiza una mayor productividad. Para que ello suceda es necesario cumplir varios requisitos, entre ellos: contar con un conocimiento de los procesos de la Oficina y una adecuada capacitación en las tecnologías de la información que los soportan.

Los ingresos de una organización y su rentabilidad se correlacionan de forma positiva con la cantidad de capacitación que se proporciona a sus empleados, ya que se les proporciona conocimientos, se desarrollan habilidades y modifican actitudes del personal de todos los niveles, para el mejorar desempeño del trabajo, a través del mejor uso de Hardware, software y la infraestructura de TI.

En relación a lo mencionado, se hace relevante efectuar una auditoría al proceso de formación de usuarios en el uso de los sistemas de información, que permitan obtener evidencia respecto a la eficacia del funcionamiento de este proceso, para identificar debilidades u oportunidades de mejora.

III. Procesos, tareas y/o temas a evaluar

Proceso de capacitación
Proceso de gestión del conocimiento
Revisión de los contenidos de las capacitaciones
Inventario de problemas y su relación con la capacitación

IV. Objetivos, alcance y periodo de la auditoría

4.1. Objetivo de la Auditoría

Determinar si la Entidad cuenta con un plan de capacitación del personal en el uso de los sistemas de información

4.2 Objetivos de Control de la Auditoría

- Comprobar si la Entidad cuenta con un presupuesto anual para capacitación
- Investigar si existe un plan de la capacitación y de desarrollo profesional de los miembros del personal de TI y/o de los usuarios del software.
- Comprobar si el contenido de los cursos cuenta con un nivel de detalle, acorde con las necesidades de los usuarios.
- Comprobar si la Entidad cuenta con un proceso de Administración del conocimiento por persona.
- Revisar la documentación que tiene el área de soporte (sistemas), e identifique el inventario de problemas, donde la causa raíz sea la capacitación.

4.3 Criterios de la auditoría

- Manual de Organización y Funciones, vigentes desde el 10 de octubre de 2011
- Reglamento de Organización y Funciones, vigentes desde el 20 de mayo de 2011.
- Reglamento de Trabajo del Personal, vigentes desde enero de 2012.
- TUO, aprobado en diciembre de 2016.
- Políticas debidamente aprobadas y vigentes.
- Lineamientos debidamente aprobados y vigentes.

4.4 Alcance de la auditoría

La materia examinada comprendió las actividades ejecutadas por el Área Informática y el Área de Recursos Humanos de la Entidad, en el marco del proceso de capacitación del personal de las diversas Áreas.
La auditoría fue realizada de acuerdo a lo dispuesto en las Normas Generales de Control Gubernamental, y la normativa interna y externa a la que está sujeta la Entidad.
La auditoría se realizó en la Oficina Principal, en la ciudad de Piura.

4.5 Periodo a examinar

Período comprendido desde el 01 de enero de 2018 al 30 de setiembre de 2018.

V. Especialistas que participan en la auditoría

La comisión auditora está conformada por:

PERSONAL NECESARIO

CARGO	PROFESION	ESPECIALIDAD
Supervisor	Ing. Informático	Capacitación
Especialista 1	Ing. Informático	Capacitación
Jefe de Comisión	Ing. Informático	Capacitación
Especialista 2	Administrador	Capacitación
Integrante	Ing. Informático	Documentador

Elaboración propia

VI. Administración de recursos

6.1. Presupuesto de tiempo

Tiempo estimado por etapas

ACTIVIDADES	DIAS UTILES	TOTAL PERSONAS	DIAS CALENDARIO	
			DEL 05/11/2018	AL 14/12/2018
PLANIFICACION	5	2	DEL 05/11/2018	AL 09/11/2018
EJECUCIÓN	15	3	DEL 12/11/2018	AL 30/11/2018
COMUNICACIÓN DE DEFICIENCIAS O FALLAS	5	2	DEL 03/12/2018	AL 07/12/2018
EVALUACION DE DESCARGOS	2	1	DEL 10/12/2018	AL 11/12/2018
REDACCION DE INFORME	2	2	DEL 12/12/2018	AL 13/12/2018
SUSTENTO Y ELEVACION DE INFORME	1	1	DEL 14/12/2018	AL 14/12/2018
TOTAL DIAS UTILES	30			

Elaboración propia

Horas Hombre Programadas

CARGO	PLANIFICACIÓN	EJECUCIÓN	COMUNICACIÓN DE DEFICIENCIAS	EVALUACIÓN DE DESCARGOS	REDACCIÓN DEL INFORME	SUPERVISIÓN SUSTENTACIÓN Y ELEVACIÓN DE INFORME	TOTAL HORAS HOMBRE
Supervisor	40	30					70
Auditor/Jefe Comisión	40	14	40	16	16	8	134
Especialista 1/ Informático		120					120
Especialista 2/ Administrador		120					120
Documentador			40		16		56
TOTALES	80	284	80	16	32	8	500

6.2. Costo de la auditoría

El costo que demanda el desarrollo de la Auditoria es de S/ 28,000.00 (Veintiocho mil con 00/100 soles).

6.3. Fecha de entrega del informe de auditoría

Se emitirá un informe en el cual se expondrán los resultados del Examen Especial. La fecha de entrega del informe está prevista para el 28/02/2019.

6.4. Contenido propuesto del informe de auditoría

I. Presentación
II. Definición, objetivos y ámbito
III. Enumeración de temas
IV. Análisis
V. Conclusiones
VI. Recomendaciones
VII. Plan de Implementación
VIII. Beneficios
IX. Plan de seguimiento y control

4.2.2. FASE DE EJECUCIÓN – PAPELES DE TRABAJO

PAPEL DE TRABAJO
AUDITORIA DE SISTEMAS

Unidad Administrativa: Área de Informática y Recursos Humanos
Elaboró: LP
Referencia: PT001
Revisó: HR
Cédula: Presupuesto de Capacitación

Objetivo de Control:
Comprobar si la Entidad cuenta con un presupuesto anual para capacitación

Procedimiento:
- ✓ Verifique que este se encuentre debidamente aprobado.
- ✓ Verifique si se considera un rubro específico de capacitación en Sistemas de información (SI).
- ✓ Verifique en los informes mensuales de ejecución presupuestaria, el uso del presupuesto asignado a capacitación de SI.

Observaciones:

Situación Real:
Para el desarrollo del procedimiento se utilizaron las siguientes técnicas y pruebas de auditoria.

<u>Técnicas</u>:

- ✓ Revelamiento: Es una técnica que consiste en recopilar información que permita comprender integralmente el funcionamiento de un sistema, proceso, actividad o materia a examinar, proporcionando un compendio de información específica que sustente el proceso de la auditoría con criterios racionales.

- ✓ Comprobación: Es la técnica que permite al auditor corroborar la existencia, legalidad, integridad y legitimidad de las operaciones realizadas o transacciones registradas en los sistemas de información, mediante la verificación de los documentos que la justifican o sustentan, los mismos que son proporcionados por la entidad auditada, y sirven de sustento para la opinión del auditor.

Pruebas de auditoria:

Con oficio n.° 004-2018-AA/LP del 12 de noviembre de 2018, se solicitó al jefe del Área de Sistemas, la evidencia correspondiente sobre el requerimiento de presupuesto efectuado para el Plan 2018.

Asimismo, con oficio n.° 003-2018-AA/LP de 12 de noviembre de 2018, se solicitó al jefe del área de presupuesto y planificación, el presupuesto de capacitación del personal de la Entidad, respecto del año 2018, y su correspondiente informe de ejecución al 31 de agosto de 2018.

Mediante carta n.° 073-2018-SUNARP/SIS de 19 de noviembre de 2018, el jefe de Sistemas adjunta documentación respecto a su gestión de requerimiento de asignación presupuestaría para capacitación en sistemas de información en el año 2018.

Mediante carta n.° 010-2018-SUNARP/P. P de 18 de noviembre de 2018, el jefe de presupuesto y planificación, alcanzó el presupuesto correspondiente al año 2018, y su respectivo informe de ejecución al 31 de agosto de 2018, donde se aprecian lo siguiente:

- Se cuenta con un presupuesto aprobado de capacitación de personal para el año 2018, por el importe de:

S/ 200 000,00 soles, el cual incluye el pago de capacitadores nacionales e internacionales. En este presupuesto si se considera el rubro de capacitación en Sistemas de información por el importe de S/ 50 000,00. Asimismo, se evidencia que este documento de gestión si cuenta con la aprobación del Gerente de Administración y el Titular de la Entidad.

- El informe mensual de evaluación de gastos y ejecución presupuestaría al 31 de agosto de 2018, muestra que se ha gastado S/ 100 000, 00 soles, los cuales han sido destinado para gastos de representación; siendo evidente que parte del importe presupuestado para capacitación en el año 2018, fue destinado para otros fines distintos a lo programado. Respecto al gasto de capacitación en sistemas de información se evidencia que se ha gastado solo S/5 000,00, los cuales se sustentan con facturas sobre de 2 eventos.

Situación Prevista:
La Entidad debe aprobar el presupuesto suficiente para capacitación y desarrollo de su personal, el cual no será destinado para otro tipo de gastos, bajo responsabilidad. Esta disposición se encuentra establecida en el Estatuto de la Entidad, vigente desde el 2010, donde en su artículo 200° se detalla lo referido a la capacitación del personal.

El presupuesto anual debe ser elaborado por el Jefe del Área de Presupuesto y planificación, quien debe presentarlo para la aprobación por parte del Gerente de Administración y el Titular de la Entidad, tal como lo establece el MOF y el TUO de la Entidad.

Asimismo, es responsabilidad del Jefe del Área de Presupuesto de emitir informes mensuales sobre la ejecución del gasto y la evaluación presupuestaria de la Entidad, tal como se establece en su MOF.

De acuerdo al MOF del Jefe de Sistemas, se identifica que este funcionario es el responsable de plantear las necesidades de capacitación en Sistemas de información y gestionar su incorporación en el presupuesto anual de la Entidad.

Conclusión:

Se advierte que la Entidad cuenta con un presupuesto anual de capacitación para el año 2018 por el importe de S/ 200 000,00, el cual fue aprobado por los funcionarios correspondientes; donde se evidencia un rubro para gastos por capacitación en sistemas de información por el importe de S/ 50 000,00.

Al 31 de agosto de 2018, ya se han pagado S/ 100 000,00 en gastos de representación, que son fines diferentes a los presupuestados, situación que debe ser aclarado por los funcionarios responsables.

Al 31 de agosto de 2018, solo se ha gastado S/ 5 000,00 de los S/ 50 000,00 presupuestados, en dos eventos de capacitación de sistemas de información, situación que debe ser aclarado por los funcionarios responsables.

Recomendación:

Se recomienda al Titular de la Entidad:

- Disponer que se gestione el uso de los recursos presupuestados para capacitación, y de ser necesario se reestructure, con la finalidad de efectuar capacitaciones prioritarias en lo que queda del año 2018.
- Reiterar a los funcionarios correspondientes, el uso adecuado de los recursos presupuestados.
- Disponer que se inicie los procesos administrativos y/o legales, sobre los que resulten responsables del uso de los recursos presupuestados para capacitación para otros fines.

Elaboró: LP	Supervisó: HR
Fecha: 20 de noviembre de 2018	Fecha: 21 de noviembre de 2018

PAPEL DE TRABAJO
AUDITORIA DE SISTEMAS

Unidad Administrativa: Área de Recursos Humanos
Elaboró: LP
Referencia: PT002
Revisó: HR
Cédula: Plan de capacitación

Objetivo de Control:
Investigar si existe un plan de la capacitación y de desarrollo profesional de los miembros del personal de TI y/o de los usuarios del software.

Procedimiento:
- ✓ Verifique si existe el plan de capacitación y de desarrollo profesional de los miembros del personal de TI y/o de los usuarios del software.
- ✓ Verifique si existe el programa de capacitación y de desarrollo profesional de los miembros del personal de TI y/o de los usuarios del software.

Observaciones:

Situación Real:

Para el desarrollo del procedimiento se utilizaron las siguientes técnicas y pruebas de auditoria.

Técnicas:

- ✓ Revelamiento: Es una técnica que consiste en recopilar información que permita comprender integralmente el funcionamiento de un sistema, proceso, actividad o materia a examinar, proporcionando un compendio de información específica que sustente el proceso de la auditoría con criterios racionales.

- ✓ Comprobación: Es la técnica que permite al auditor corroborar la existencia, legalidad, integridad y legitimidad de las operaciones realizadas o transacciones registradas en los sistemas de información, mediante la verificación de los documentos que la justifican o sustentan, los mismos que son proporcionados por la entidad auditada, y sirven de sustento para la opinión del auditor.

- ✓ Indagación: Consiste en la búsqueda de información apropiada, a través de personas bien informadas tanto de dentro como de fuera de la entidad. La indagación se utiliza de forma extensiva a lo largo de la auditoría y adicionalmente a otros procedimientos.

Pruebas de auditoria

- ✓ Con oficio n.° 005-2018-AA/LP de 17 de noviembre de 2018, se solicitó a la comisión especial, la propuesta del plan de capacitación y de desarrollo profesional de los miembros del personal de TI y/o de los usuarios del software.

- ✓ Con oficio n.° 006-2018-AA/LP de 17 de noviembre de 2018, se solicitó al Directorio de la Entidad, el plan de capacitación y de desarrollo profesional de los miembros del personal de TI y/o de los usuarios del software.

- ✓ Con oficio n.° 007-2018-AA/LP de 17 de noviembre de 2018, se solicitó a la comisión especial, el programa de capacitación del personal de TI y demás usuarios del Software.

- ✓ El Gerente General encargado de la aprobación del plan de capacitación, a través de la carta n.° 001-2018-SUNARP/GG de 20 de noviembre de 2018, señaló que: "(…) la comisión especial encargada de la elaboración de la propuesta de capacitación, no la presentó al Directorio para su aprobación, por lo que a la fecha no existe un plan de capacitación del personal en TI (…)"

  Pese a los oficios reiterativos, la comisión especial no dio respuesta al requerimiento de información realizada por la comisión auditora.

Situación Prevista:

La Entidad a través de una comisión conformada por personal de TI, Presupuesto y Administración, elaboraran un pan de capacitación y de desarrollo profesional de todo el personal de TI y demás usuarios de software de registro de información, la misma que será aprobada por el directorio de la entidad conforme a lo establecido en el artículo 151° del **Estatuto de la Entidad, vigente desde el 2010, se tiene que:** "(…) la entidad aprobará un plan de capacitación y de desarrollo profesional de todo los usuarios que utilicen software de registro de información; la capacitación de los miembros del personal de TI es obligatoria.

La formulación de la propuesta del plan de capacitación, es de exclusiva responsabilidad de la comisión especial, conformada por personal de TI, Presupuesto y Administración, quienes deberán presentarla a más tardar, la primera quincena del mes de marzo de todos los años, conforme lo establecen el **Manual de Organizaciones y Funciones y Texto Único Ordenado de la Entidad.**

El Directorio de la Entidad, contará con 15 días de presentada la propuesta del plan de capacitación para su aprobación, conforme el artículo 80° del **Manual de Organización y Funciones de la Entidad.**

Una vez aprobado el plan de capacitación, es responsabilidad de la comisión, de establecer los mecanismos para su ejecución, conforme lo señala el Estatuto de la Entidad.

Conclusión:
Se evidenció que la Comisión Especial, encargada de elaborar la propuesta de capacitación del personal de la Entidad en TI, no la presentó al Directorio para su aprobación, pese a lo normado en los documentos de gestión.

Recomendación:
Se recomienda al Titular de la Entidad:

- ✓ Monitorear el cumplimiento de lineamientos y política previamente establecidas
- ✓ Sancionar al personal responsable, por el incumplimiento de funciones.
- ✓ Requerir la elaboración y aprobación del plan de capacitación del personal de la entidad en TI, pese al tiempo transcurrido.

Elaboró: LP	**Supervisó:** HR
Fecha: 21 de noviembre del 2018	**Fecha:** 22 de noviembre del 2018

PAPEL DE TRABAJO
AUDITORIA DE SISTEMAS

Unidad Administrativa: Área de Recursos Humanos y Área de Informática
Elaboró: LP
Referencia: PT003
Revisó: HR
Cédula: Temas de capacitación

Objetivo de Control:
Comprobar si el contenido de los cursos cuenta con un nivel de detalle, acorde con las necesidades de los usuarios.

Procedimiento:
- ✓ Verifique la existencia de procedimientos para solicitud de cursos capacitación.
- ✓ Verifique que los sílabos de los cursos cuenten con un nivel de detalle acorde a las necesidades de los usuarios internos, donde se considere: listado de los temas a tratar, usuarios objetivo, frecuencia y horarios de clase, fuente de capacitación, responsable de capacitación.
- ✓ Verifique que los cursos se dictaron según el detalle establecido en los sílabos.
- ✓ Verifique si el personal del Área de Sistemas fue capacitado en temas especializados y acorde con los sistemas de información de la Entidad.

Observaciones:

Situación Real:
Para el desarrollo del procedimiento se utilizaron las siguientes técnicas y pruebas de auditoria.

<u>Técnicas</u>:

- ✓ Revelamiento: Es una técnica que consiste en recopilar información que permita comprender integralmente el funcionamiento de un sistema, proceso, actividad o materia a examinar, proporcionando un compendio de información específica que sustente el proceso de la auditoría con criterios racionales.

- ✓ Comprobación: Es la técnica que permite al auditor corroborar la existencia, legalidad, integridad y legitimidad de las operaciones realizadas o transacciones registradas en los sistemas de información, mediante la verificación de los documentos que la justifican o sustentan, los mismos que son proporcionados por la entidad auditada, y sirven de sustento para la opinión del auditor.

- ✓ Entrevista: Es la técnica por medio de la cual se obtiene información complementaria que sirve más como apoyo que como evidencia directa del

examen que se realiza. Se aplica a través de preguntas directas, formales o informales, al personal que labora en el área auditada o a terceros, cuyas actividades guardan relación con las operaciones de esta.

Pruebas de auditoria:

Con oficio n.° 014-2018-AA/LP del 21 de noviembre de 2018, se solicitó al jefe de recursos humanos, el listado de cursos internos y externos brindados al personal de la Entidad entre el 01 de enero de 2018 al 31 de agosto de 2018, adjuntado los sílabos y/o contenido de los cursos. Asimismo, se solicitó la remisión del Procedimiento aprobado donde se indique el proceso a seguir para la solicitud y aprobación de los cursos de capacitación.

Mediante carta n.° 073-2018-SUNARP/PER de 22 de noviembre de 2018, el jefe del área de recursos humanos adjunta el detalle de los cursos dictados relacionados a sistemas de información, donde se aprecia lo siguiente:

- Que a la fecha aún no se cuenta con un plan de capacitación integral del personal de la entidad; y siendo una de las prioridades fundamentales, en los próximos días se dispondrá la elaboración y aprobación de dicho plan, ya que se ha previsto recursos suficientes para su ejecución.

- A la fecha no se cuentan con un Procedimiento formal que indique los pasos a seguir para la solicitud de cursos de capacitación.

- En el listado de cursos remitidos, solo se aprecia 02 cursos externos relacionados a Sistemas de Información, brindados al Jefe y un analista del Área de Sistemas.

Al respecto la comisión auditora se entrevistó con el Jefe y el analista del Área de sistemas, para conocer los alcances del contenido de los cursos externos y verificar el material recibido en los cursos. Sobre el particular se evidencia que en uno de ellos se impartió conocimiento en herramientas de diseño e implementación de software, los mismos que están acorde con las necesidades en la Institución. En relación al otro curso se evidencia que, comprendió la capacitación en lenguajes de programación, el cual no se usa en la Entidad; por lo que se considera que esta capacitación no tendría los beneficios esperados. Al respecto la comisión auditora se entrevistó con el jefe del área de recursos humanos, quien manifestó que él solo autorizó la inscripción y asistencia al curso solicitado por el área de sistemas, pero que no tiene la capacidad técnica para saber si el contenido está alineado con la tecnología que dispone la Entidad, ni tampoco exigió un informe sustentado sobre ello.

Adicionalmente, la comisión auditora, entrevisto a 02 personas del Área de Sistemas y 02 personas de las Áreas de soporte, con la finalidad de percibir y

obtener información adicional sobre el proceso de capacitación, obteniéndose el siguiente resultado:

- Las personas manifestaron que no se tienen claridad sobre las capacitaciones que recibirán en el año en curso.
- No se ha dictado cursos de capacitación internos sobre el uso de los sistemas de información.
- No tienen idea cual es el procedimiento usado para solicitar un curso de capacitación.

Situación Prevista:

La Entidad debe aprobar un plan de capacitación y de desarrollo profesional de todos los usuarios que utilicen software; la capacitación de los miembros del personal de TI será obligatoria. Esta disposición se encuentra establecida en el Estatuto de la Entidad, vigente desde el 2010, donde en su artículo 151° se detalla lo referido a la capacitación del personal.

El área de recursos humanos y área de sistemas serán los encargados de proponer y presupuestar cursos de capacitación en sistemas de información, tanto a los usuarios internos como al personal del Área de Sistemas, los mismos deberán contar con sílabos acorde con las necesidades de capacitación. Ésta responsabilidades se encuentra en el Reglamento de capacitación de la Entidad.

Conclusión:

Se advierte que, en la Entidad, en el año 2018, no cuenta con un plan de capacitación y de desarrollo profesional de los miembros del personal de TI y/o de los usuarios del software, por lo tanto, no cuenta una estructura clara sobre los contenidos de los cursos.

No se cuenta con un procedimiento para solicitar y aprobar un curso de capacitación.

No se ha dictado cursos de capacitación sobre el uso de los sistemas de información.

Recomendación:

- Elaborar un Plan integral de capacitación, donde se considere entre otros puntos, una estructura clara sobre los contenidos de los cursos.

- Se implemente un Procedimiento formal para solicitar y aprobar un curso de capacitación, donde se considere entre otros temas: un informe técnico de la factibilidad y beneficios del curso, el flujo de aprobación y las actividades de retroalimentación o réplica del participante sobre sus compañeros.

Elaboró: LP	**Supervisó:** HR
Fecha: 23 de noviembre del 2018	**Fecha:** 24 de noviembre del 2018

PAPEL DE TRABAJO
AUDITORIA DE SISTEMAS

Unidad Administrativa: Área de Recursos Humanos
Elaboró: LP
Referencia: PT004
Revisó: HR
Cédula: Administración del conocimiento

Objetivo de Control:
Comprobar si la Entidad cuenta con un proceso de Administración del conocimiento por persona.

Procedimiento:
- ✓ Verifique si la Entidad tiene un procedimiento formal para la evaluación de conocimiento de las personas.
- ✓ Verifique si existe concentración de cursos de capacitación sobre el personal.
- ✓ Verifique si la Entidad cuenta con un repositorio físico o electrónico sobre las capacitaciones brindadas al personal, y comprobar que este se encuentre actualizado.

Observaciones:

Situación Real:

<u>Técnicas</u>:

- ✓ Revelamiento: Es una técnica que consiste en recopilar información que permita comprender integralmente el funcionamiento de un sistema, proceso, actividad o materia a examinar, proporcionando un compendio de información específica que sustente el proceso de la auditoría con criterios racionales.

- ✓ Comprobación: Es la técnica que permite al auditor corroborar la existencia, legalidad, integridad y legitimidad de las operaciones realizadas o transacciones registradas en los sistemas de información, mediante la verificación de los documentos que la justifican o sustentan, los mismos que son proporcionados por la entidad auditada, y sirven de sustento para la opinión del auditor.

- ✓ Cuestionario: Es una técnica que utiliza el auditor para obtener información por medio de preguntas escritas organizadas, que deben ser contestadas por los funcionarios o empleados de la entidad, puede abarcar aspectos cuantitativos y cualitativos.

Pruebas de auditoria:

Con oficio n.° 015-2018-XYZ/CA del 22 de noviembre de 2018, se solicitó al Área de recursos humanos:

- Los files de 20 personas de la Entidad, de las áreas de sistemas y áreas operativas.
- Un reporte actualizado con el listado de cursos brindados a éstas 20 personas en los 2 últimos años.
- Sustento de las evaluaciones de conocimientos aplicadas al personal, sobre el uso de los sistemas de información de la Entidad.

Mediante carta n.° 074-2018-SUNARP/PER de 25 de noviembre de 2018, el Área de recursos humanos respondió al oficio. La comisión auditora, luego de analizar la información aprecia lo siguiente:

- Los files de 10 de las 20 personas se encuentran desactualizados, ya que no se adjuntan las constancias de los cursos asistidos.
- A pesar de que en el sistema se cuenta con las opciones para registrar información sobre los cursos recibidos por cada persona, estas no se utilizan siempre, en vista que, del listado alcanzado por el Área de recursos humanos, no se contempla la información de los cursos asistidos para 6 personas.
- No se han realizado evaluaciones de conocimientos sobre el uso de los sistemas de información.
- 02 personas han recibido 5 cursos de capacitación en el año 2017, 8 de ellas han recibido 1 capacitación y 12 de ellas no han recibido capacitación; con lo cual se evidencia que existe una concentración de capacitación en solo algunas personas.

El equipo auditor considero aplicar a una muestra de 20 personas, un Cuestionario que tuvo como objetivo identificar el grado de conocimiento sobre el uso de los sistemas de información, del cual se obtuvo que: 6 personas tienen conocimiento aceptable sobre el uso de los sistemas de información, 11 personas tienen un conocimiento limitado y 3 de ellas nos respondieron el cuestionario. De lo cual se evidencia el alto grado de desconocimiento del personal en el uso de los sistemas de información.

Situación Prevista:

De acuerdo con lo planteado en el Reglamento interno de trabajo, se establece que la Entidad brindará capacitación a su personal sobre los procedimientos internos y el uso adecuado de los recursos.

Asimismo, de acuerdo con el ROF, se establece la responsabilidad del Área de recursos humanos de gestionar las capacitaciones del personal y llevar a cabo un control de los files de los mismos, apoyándose en los recursos físicos o electrónicos con que cuentan

Conclusiones:

No se administra adecuadamente la información de los cursos recibidos por el personal, dado que:

- Existen files del personal desactualizados respecto a la información de cursos.
- No se registra en el Sistema la totalidad de capacitaciones recibidas por el personal.

No se cuentan con un procedimiento formal para las evaluaciones de conocimientos al personal, sobre el uso de los sistemas de información.

Existe concentración de capacitación en algunos trabajadores, con lo cual no se distribuye adecuadamente el conocimiento.

Existe un conocimiento limitado por parte del personal, en el uso de los sistemas de información.

Recomendaciones:

Se recomienda al titular de la Entidad:

- Disponer que el área de recursos humanos actualice los files del personal, y registre en el sistema la información de las capacitaciones recibidas por el personal. Y se reitere que en lo sucesivo se realice esta labor.
- Efectuar evaluaciones periódicas al personal sobre sus conocimientos en el uso de los sistemas de información. Y el resultado de ello se adjunte en su legajo personal.

- Se elabore un plan integral de capacitación, donde se contemple capacitaciones para todo el personal, evitando la concentración de estas en pocos trabajadores.

Elaboró: LP	**Supervisó:** HR
Fecha: 26 de noviembre del 2018	**Fecha:** 27 de noviembre del 2018

PAPEL DE TRABAJO
AUDITORIA DE SISTEMAS

Unidad Administrativa: Oficina de Informática
Elaboró: LP
Referencia: PT005
Revisó: HR
Cédula: Documentación

Objetivo de Control:
Revisar la documentación que tiene el área de soporte (sistemas), e identifique los inventarios de problemas, donde la causa raíz sea la capacitación.

Observaciones:

Situación Real:

Para el desarrollo del procedimiento se utilizaron las siguientes técnicas y pruebas de auditoria.

Técnicas:

- ✓ Inspección, en el examen que se realiza a bienes, obras, registros, documentos y valores de la entidad, para constatar su existencia y autenticidad.

- ✓ Revelamiento: Es una técnica que consiste en recopilar información que permita comprender integralmente el funcionamiento de un sistema, proceso, actividad o materia a examinar, proporcionando un compendio de información específica que sustente el proceso de la auditoría con criterios racionales.

- ✓ Indagación: Consiste en la búsqueda de información apropiada, a través de personas bien informadas tanto de dentro como de fuera de la entidad. La indagación se utiliza de forma extensiva a lo largo de la auditoría y adicionalmente a otros procedimientos.

- ✓ Entrevista: Técnica por medio de la cual se obtiene información complementaria que sirve más como apoyo que como evidencia directa del examen que se realiza.

- ✓ Observación: Consiste en presenciar un proceso o un procedimiento realizado por otras personas.

Pruebas de auditoria

Con fecha, 25 de noviembre de 2018, la comisión auditora, se apersonó al área de soporte, quienes identificaron los siguientes problemas:

- No se evidenció manuales o guías del software LXC.
- De todo el personal que labora en dicha área, el único que sabe utilizar todas las opciones del software, es el jefe, puesto que el resto de personal, ante las preguntas de la comisión auditoria, sobre el manejo de ciertas funciones no respondían, o para responderlas consultaban con su jefe.
- Ante la pregunta, ¿cada que tiempo vienen recibiendo capacitaciones respecto del uso de software?, la mayoría respondió que no han recibido capacitación por parte de la Entidad; otros respondieron que solo recibieron capacitación cuando instalaron por primera vez el software en la entidad.
- Ante la pregunta, ¿Cómo solucionan un determinado problema que se presente en el uso del software por parte de usuarios que no sean de soporte?; la respuesta fue que consultaba con su jefe para darle solución.

El jefe de la referida área, sostuvo en varias oportunidades de manera verbal solicitó la implementación de un plan de capacitación, en cuanto al uso de software; sin embargo nunca tuvo respuesta por parte de la alta dirección, razón por la cual, no se ha capacitado al personal de TI, ni mucho menos al personal usuario del programa.

Situación Prevista:

Cada área funcional de la Entidad, debe custodiar y preservar la información que le corresponda, conforme establecen los documentos de gestión de la Entidad.

En ese sentido, se advierte que el área de soporte, tiene la obligación de la custodia y preservación de los documentos de los diferentes programas de TI.

Conclusión:

De la revisión a la documentación que tiene el área de soporte, se evidenció que no cuenta con manuales o guías respecto del software que utiliza la entidad para el registro de información tanto interna como externa; asimismo se determinó que el personal de dicha área, no cuanta con la debida capacitación sobre el manejo de todas las opciones que ofrece el referido software.

Así también, se determinó la poca voluntad por parte de la alta dirección de la entidad por implementar un plan de capacitación y de desarrollo profesional de sus colaboradores, pese al presupuesto que inicialmente se destina.

Recomendación:

Se recomienda al Titular de la Entidad:

- Implementar con mobiliario adecuado para la preservación, conservación y custodia de la documentación correspondiente.
- Reglamentar que durante un plazo determinado las áreas de la Entidad conserven la información bajo responsabilidad.

Elaboró: LP	**Supervisó:** HR
Fecha: 30 de noviembre del 2018	**Fecha:** 30 de noviembre del 2018

4.2.3. FASE DE INFORME DE AUDITORIA

Esta fase de auditoría, tiene como resultado una síntesis, de lo trabajado en las dos fases anteriores, razón por la cual sólo se desarrollan los ítems del informe que corresponden a: plan de implementación, los beneficios y el plan de seguimiento y control considerados por el auditor de sistemas, por cada objetivo de control.

A continuación, se indican las acciones sugeridas por el auditor para cada objetivo de control desarrollado.

Objetivo de Control: Comprobar si la Entidad cuenta con un presupuesto anual para capacitación **Plan de Implementación**
Acciones que realizará la Entidad: - El Jefe de Sistemas realizará una priorización de los temas de capacitación. - La Gerencia de Administración reestructurará el presupuesto de capacitación, y tomará medidas para que se realice las capaciones prioritarias planteadas por el Jefe de Sistemas. - Se emitirá un memorando de reiteración a los funcionarios relacionados a tema de presupuesto y capacitación, para cumplan con sus funciones. - La Gerencia de Administración solicitará los descargos correspondientes a los responsables del uso inadecuado de los recursos, y ser necesario tomará las medidas administrativas y/o legales correspondientes. **Responsable de las acciones:** Jefe de Sistemas y Gerencia de Administración. **Fecha propuesta de implementación:** 03 de enero de 2019.

Beneficios
- En el breve plazo: En lo que queda del año 2018, se podrá realizar capacitaciones en Sistemas de información. - En el medio y largo plazo: se podrá contar con un presupuesto de capacitación de sistemas de información priorizado. Además, se podrá contar con funcionarios concientizados en el uso adecuado de los recursos de capacitación.
Plan de seguimiento y control
Producto : Informe de la Gerencia de Auditoria - Seguimiento de la implementación de recomendación **Dirigido a :** Titular de la Entidad **Frecuencia :** Bimestral

Objetivo de Control: Investigar si existe un plan de la capacitación y de desarrollo profesional de los miembros del personal de TI y/o de los usuarios del software. **Plan de Implementación**
Acciones que realizará la Entidad: Conformar una comisión especial, encargada de elaborar la propuesta del plan de capacitación Responsable de las acciones: Gerentes de Tecnología de Información, Planificación y Administración **Fecha propuesta de implementación:** 30 de noviembre de 2018
Beneficio
✓ Contar con un plan de capacitación y de desarrollo profesional de los miembros del personal de TI y/o de los usuarios del software

Plan de seguimiento y control
Producto : Informe de la Gerencia de Auditoria - Seguimiento de la implementación de recomendación **Dirigido a :** Titular de la Entidad **Frecuencia :** Trimestral
Objetivo de Control: Comprobar si el contenido de los cursos cuenta con un nivel de detalle, acorde con las necesidades de los usuarios. **Plan de Implementación**
Acciones que realizará la Entidad: Se formará un Comité técnico, que lo presidirá el Gerente de Administración, para la elaboración de un Plan integral de capacitación. **Responsable de las acciones:** Gerencia de Administración, Jefe del área de recursos humanos, jefe del área de Sistemas y Jefe de presupuesto y planificación. **Fecha propuesta de implementación:** 30 de noviembre de 2018
Beneficios
- Trazabilidad de los cursos de capacitación a dictarse en el año. - Trazabilidad de los conocimientos impartidos en cursos - Cursos enfocados a las necesidades de la Entidad - Proceso claro para la solicitud y aprobación de cursos de capacitación
Plan de seguimiento y control
Producto : Informe de la Gerencia de Auditoria - Seguimiento de la implementación de recomendación

Dirigido a : Titular de la Entidad
Frecuencia : Trimestral

Objetivo de Control:

Comprobar si la Entidad cuenta con un proceso de Administración del conocimiento por persona.

Plan de Implementación

Acciones que realizará la Entidad:

- Respecto a los cursos de capacitación, se actualizará los files del personal y se registrará la información en los sistemas.

- Se elaborará un plan integral de capacitación donde se contemple: las capacitaciones al personal y las evaluaciones periódicas sobre el uso de los sistemas de información

Responsable de las acciones: Gerencia de Administración y jefe de recursos humanos

Fecha propuesta de implementación: 30 de noviembre de 2018

Beneficios

- Se contará con un procedimiento formal para la evaluación de conocimiento de las personas.

- La capacitación será equitativa para todo el personal

- Se contará con un repositorio físico o electrónico sobre las capacitaciones brindadas al personal, donde se pueda evidenciar el nivel que tiene cada uno de ellos.

Plan de seguimiento y control
Producto : Informe de la Gerencia de Auditoria - Seguimiento de la implementación de recomendación **Dirigido a :** Titular de la Entidad **Frecuencia :** Trimestral

Objetivo de Control: Revisar la documentación que tiene el área de soporte (sistemas), e identifique los inventarios de problemas, donde la causa raíz sea la capacitación. **Plan de Implementación**
Acciones que realizará la Entidad: - Disponer que el área de administración, a través del área de abastecimientos, implementen con mobiliario a las áreas de la Entidad para la preservación y custodia de la información. - Realizar visitas inopinadas a las respectivas áreas con la finalidad de verificar la adecuado custodia y preservación de la información **Responsable de las acciones:** Gerentes de Administración y Planificación **Fecha propuesta de implementación:** 30 de noviembre de 2018
Beneficio
✓ Conservación y custodia de la información en óptimas condiciones
Plan de seguimiento y control
Producto : Informe de la Gerencia de Auditoria - Seguimiento de la implementación de recomendación **Dirigido a :** Titular de la Entidad **Frecuencia :** Trimestral

CONCLUSIONES

Y

RECOMENDACIONES

CONCLUSIONES

1) Se desarrolló con éxito la propuesta de un modelo de auditoría de sistemas de información que ayude a las acciones de control en una auditoría de TIC para una entidad pública, como muestra de ello se aplicó con éxito el modelo en la Oficina de SUNARP – Otuzco, con lo cual se demostrado la hipótesis planteada en la investigación.

2) Para lograr tener éxito en el desarrollo del modelo propuesto, ha sido importante conocer y comprender el funcionamiento de la organización pública de forma general, sus normas, políticas y procedimientos más importantes relacionados a los sistemas de información, así como, lo establecido por la Contraloría General de la República, ente rector del Sistema Nacional de Control. Del mismo modo se ha tomado como referencia lo establecido por la Norma Técnica Peruana 17799 y algunos marcos de referencia como la ISO 27001 y COBIT.

3) En el desarrollo del modelo propuesto, específicamente en el formato del Plan de Auditoría propuesto, se ha dejado claro que existen los objetivos de la auditoría, los cuales indican el fin persigue la entidad pública que requiere hacer la auditoría o el titular de la misma que la solicita.

4) En el desarrollo del modelo propuesto, se establecen los objetivos de control de la auditoría, los cuales forman la parte operativa de la misma que se realiza sobre la entidad pública, estos objetivos se definen en el modelo del Plan de Auditoría propuesto, y su objetivo es evaluar los controles existentes o identificar la ausencia de ellos dentro del entorno de los sistemas de información.

5) En el desarrollo del modelo de programa de auditoría propuesto, se traslada la operacionalización de los objetivos de control, mediante acciones concretas y objetivas, definidas como procedimientos de auditoría, los cuales indican las secuencias de tareas o actividades a realizar para encontrar las deficiencias de los controles existentes o simplemente la carencia de ellos, sobre la materia de lo que se está auditando en un sistema de información

RECOMENDACIONES

La presente tesis, es un estudio que se puede ampliar y perfeccionar con estudios posteriores, implementando otros aspectos como el desarrollo de pruebas de auditoría de sistemas de información, mejorar y ampliar los objetivos de control propuestos tomando como referencia los marcos de trabajo como COBIT o las normas ISO, tratando de adaptar lo que más se aplica a la realidad peruana, respetando lo establecido por el ente rector del Sistema Nacional de Control del Perú.

REFERENCIAS BIBLIOGRAFICAS

- ALIAGA, L (2013). **Diseño de un sistema de gestión de seguridad de información para un instituto educativo**. [Tesis]. Perú: Pontificia Universidad Católica del Perú.

- BALLER, S., DUTTA, S. & LANVIN, B. (2016). **"The Global Information Technology Report 2016".** World Economic Forum.

- BARAHONA, J Y GARZON, E (2014). **Auditoria de los riesgos informáticos en el departamento de tecnología de la empresa KUBIEC usando Cobit 4.1 y la norma ISO/IEC 27001 como marco de referencia**. [Tesis]. Ecuador: Escuela Politécnica Nacional.

- CERINI, M & PRÁ, P. (2002) Plan **de Seguridad Informática**. Trabajo para desarrollar una auditoria informática.

- CORAISACA, J (2012). **Aplicación de Cobit 4.1 en la auditoria de una aplicación informática tipo web de una institución financiera**. [Tesis]. Ecuador: Escuela Politécnica Nacional.

- ISACA - GOVERNANCE INSTITUTE. (2007). **COBIT 4.1.**

- LEY Nº 27785: **Ley Orgánica del Sistema Nacional de Control y de la Contraloría General de la República del Perú.**

- MOLINA, J Y OÑA, D (2013). **Auditoria del sistema informático de la empresa "MANUFACTURAS AMERICANAS CIA.LTDA"**. [Tesis]. Ecuador: Escuela Politécnica Nacional.

- MUÑOZ, C (2002). Auditoria en Sistemas Computacionales. México: PEARSON EDUCACION.

- RAMOS, C. (2015), **Propuesta de un plan de auditoria informática para el "sistema de información en salud" y el "aplicativo para el registro de formatos SIS" en los establecimientos de salud de la unidad ejecutora 400 en la región Piura en el año 2015.** [Tesis]. Perú: Universidad Nacional de Piura.

- Resolución de Contraloría 152-98-CG, **Manual, Guías de Planeamiento y Elaboración del Informe de Auditoría Gubernamental y las Guías de Papeles de Trabajo y del Auditado**. Perú

- Resolución de Contraloría 273-2014-CG. **Normas Generales de Control Gubernamental.** Perú

- Resolución de Contraloría 070-2018-CG. **Auditoría del Cumplimiento Derivada del Control Concurrente.** Perú

- SERVIR (2016). **Estructura y Funcionamiento del Estado Peruano.**